Filed: 12/15/2021 2:24 PM
Clerk
St. Joseph County, Indiana

STATE OF INDIANA	)	**IN THE ST. JOSEPH CIRCUIT/SUPERIOR COURT**
	) **SS:**	
ST. JOSEPH COUNTY	)	
ASPEN SPECIALTY INSURANCE COMPANY, as Subrogee of Trinity Health Corporation, and TRINITY HEALTH CORPORATION,	)	
Plaintiffs,	)	
v.	)	**CAUSE NO.** 71C01-2112-CT-000462
BLACKBAUD, INC.,	)	
Defendant.	)	

SUMMONS

THE STATE OF INDIANA TO DEFENDANT Blackbaud, Inc.

ADDRESS: c/o Corporation Service Company, 135 N. Pennsylvania St., Suite 1610, Indianapolis, IN 46204

You have been sued by the person(s) named "plaintiff", in the court stated above.

The nature of the suit against you is stated in the complaint which is attached to this summons. It also states the demand which the plaintiff has made against you.

You must answer the complaint in writing, by you or your attorney, within twenty (20) days, commencing the day after you receive this summons, (you have twenty-three (23) days to answer if this summons was received by mail), or judgment will be entered against you for what the plaintiff has demanded.

If you have a claim for relief against the plaintiff from the same transaction or occurrence, you must assert it in your written answer.

The following manner of service of summons is hereby designated:

CERTIFIED MAIL

Kirk D. Bagrowski, #23495-53
EICHHORN & EICHHORN, LLP
2929 Carlson Drive, Suite 100
Hammond, Indiana 46323
Telephone: (219) 931-0560
Facsimile: (219) 931-5370
Attorney for Petitioner/Defendant

12/15/2021

Rita L. Glenn

Clerk of the Circuit/Superior Court of St. Joseph County

BY: AS, Deputy

ST. JOSEPH COUNTY SEAL INDIANA

RETURN ON SERVICE OF SUMMONS

I hereby certify that I have served the within summons:

(1) By delivering a copy of the Summons and a copy of the complaint to the defendant, _____ on the _____ day of _____, 202__.

(2) By leaving a copy of the summons and a copy of the complaint to the defendant, _____ the dwelling place or usual place of abode of the said defendant, with a person of suitable age and discretion residing therein, namely _____.

(3) Other: _____.

Sheriff's Fees: _____

Additional _____

_____
Sheriff of St. Joseph County, Indiana

BY:_____, Deputy

CLERK'S CERTIFICATE OF MAILING

I hereby certify that on the _____ day of _____, 202__, I mailed this summons and copy of the complaint to the defendant, _____ by _____ mail, requesting a return receipt, at the address furnished by the plaintiff.

Date:_____

_____
Clerk of the Circuit/Superior Court of St. Joseph County

BY:_____, Deputy

RETURN ON SERVICE OF SUMMONS BY MAIL

I hereby certify that the attached return receipt was received by me showing that the summons and a copy of the complaint mailed to defendant _____ was accepted by the defendant on the _____ day of _____, 202__.

I hereby certify that the attached return receipt was received by me showing that the summons and a copy of the complaint was returned not accepted on the _____ day of _____, 202__.

I hereby certify that the attached return receipt was received by me showing that the summons and a copy of the complaint mailed to defendant _____was accepted by _____ on behalf of said defendant on the _____ day of _____, 202__.

_____
Clerk of the Circuit/Superior Court of St. Joseph County

BY:_____, Deputy

SERVICE ACKNOWLEDGED (When defendant accepts service in person)

A copy of the within summons and a copy of the complaint attached thereto were received by me at _____, this _____ day of _____, 202__.

_____
Signature of Defendant

Filed: 12/15/2021 2:24 PM
Clerk
St. Joseph County, Indiana

STATE OF INDIANA	)	**IN THE ST. JOSEPH CIRCUIT/SUPERIOR COURT**
	) **SS:**	
ST. JOSEPH COUNTY	)	
ASPEN SPECIALTY INSURANCE COMPANY, as Subrogee of Trinity Health Corporation, and TRINITY HEALTH CORPORATION,	)	
Plaintiffs,	)	
v.	)	**CAUSE NO.** 71C01-2112-CT-000462
BLACKBAUD, INC.,	)	
Defendant.	)	

APPEARANCE BY ATTORNEY IN CIVIL CASE

This Appearance Form must be filed on behalf of every party in a civil case.

1. The party on whose behalf this form is being filed is:
   Initiating __x__ Responding ____ Intervening ____ ; and

   the undersigned attorney and all attorneys listed on this form now appear in this case for the following parties:

   Name of party: Trinity Health Corporation

   Address of party *(see Question # 5 below if this case involves a protection from abuse order, a workplace violence restraining order, or a no-contact order)*

   EICHHORN & EICHHORN, LLP, 2929 Carlson Drive, Suite 100, P.O. Box 2275, Hammond, IN 46323
   Telephone # of party 219-931-0560

(List on a continuation page additional parties this attorney represents in this case.)

2. Attorney information for service as required by Trial Rule 5(B)(2)

   Name: Kirk D. Bagrowski Atty Number: #23495-53

   Name: Robert J. Feldt Atty Number: #16311-45

   Address: EICHHORN & EICHHORN, LLP, 2929 Carlson, Suite 100, P.O. Box 2275, Hammond, IN 46323

   Phone: 219-931-0560

FAX: 219-931-5370

Email Address: kbagrowski@eichhorn-law.com

Email Address: rfeldt@eichhorn-law.com

IMPORTANT: Each attorney specified on this appearance:

(a) certifies that the contact information listed for him/her on the Indiana Supreme Court Roll of Attorneys is current and accurate as of the date of this Appearance;

(b) **acknowledges that all orders, opinions, and notices from the court in this matter that are served under Trial Rule 86(G) will be sent to the attorney at the email address(es) specified by the attorney on the Roll of Attorneys regardless of the contact information listed above for the attorney**; and

(c) understands that he/she is solely responsible for keeping his/her Roll of Attorneys contact information current and accurate, see Ind. Admis. Disc. R. 2(A).

Attorneys can review and update their Roll of Attorneys contact information on the Courts Portal at http://portal.courts.in.gov.

3. This is a CT case type as defined in administrative Rule 8(B)(3).

4. This case involves child support issues. Yes ____ No X *(If yes, supply social security numbers for all family members on a separately attached document filed as confidential information on **light green paper**. Use Form TCM-TR3.1-4.)*

5. This case involves a protection from abuse order, a workplace violence restraining order, or a no – contact order. Yes ____ No X *(If Yes, the initiating party must provide an address for the purpose of legal service but that address should not be one that exposes the whereabouts of a petitioner.)* The party shall use the following address for purposes of legal service:

_____ Attorney's address

_____ The Attorney General Confidentiality program address (contact the Attorney General at 1-800-321-1907 or e-mail address is **confidential@atg.in.gov**).

_____ Another address (provide)

_____

This case involves a petition for involuntary commitment. Yes ____ No X

6. If Yes above, provide the following regarding the individual subject to the petition for involuntary commitment:

a. Name of the individual subject to the petition for involuntary commitment if it is not already provided in #1 above:

_____

b. State of Residence of person subject to petition: _____

c. At least one of the following pieces of identifying information:

(i) Date of Birth _____

(ii) Driver's License Number _____

State where issued _____ Expiration date _____

(iii) State ID number _____

State where issued _____ Expiration date _____

(iv) FBI number _____

(v) Indiana Department of Corrections Number _____

(vi) Social Security Number is available and is being provided in an attached confidential document Yes ____ No ____

7. There are related cases: Yes ____ No _X___ *(If yes, list on continuation page.)*

8. Additional information required by local rule:

_____

9. There are other party members: Yes ____ No_X___ *(If yes, list on continuation page.)*

10. This form has been served on all other parties and Certificate of Service is attached:

Yes___ No_x__

/s/ Kirk D. Bagrowski
Attorney-at-Law
(Attorney information shown above)

Filed: 12/15/2021 3:49 PM
St. Joseph Circuit Court
St. Joseph County, Indiana

STATE OF INDIANA ST. JOSEPH COUNTY	))SS:)	IN THE ST. JOSEPH CIRCUIT/SUPERIOR COURT
ASPEN SPECIALTY INSURANCE COMPANY, as Subrogee of Trinity Health Corporation, and TRINITY HEALTH CORPORATION, Plaintiffs, v. BLACKBAUD, INC., Defendant.	)	**CAUSE NO.** 71C01-2112-CT-000462

E-FILING APPEARANCE BY ATTORNEY IN CIVIL CASE

1. The party on whose behalf this form is being filed is:
   Initiating ___ Responding _X__ Intervening ____ ; and

   The undersigned attorney and all attorneys listed on this form now appear in this case for the following parties:

   Name of party: **Aspen Specialty Insurance Company, as Subrogee of Trinity Health Corporation**

   Address of party *(see Question # 5 below if this case involves a protection from abuse order, a workplace violence restraining order, or a no-contact order)*

   _____

(List on a continuation page additional parties this attorney represents in this case.)

2. Attorney information for service as required by Trial Rule 5(B)(2)

   Name: Michael Kreppein Atty Number: 22430-64

   Address: Wilson Elser Moskowitz Edelman & Dicker LLP
   233 E. 84th Drive – Park Tower, Suite 201
   Merrillville, IN 46410

   Phone: (219) 525-0560

   FAX: (219) 525-0561

   Email Address: Michael.kreppein@wilsonelser.com

3. This is a _CT_ case type as defined in administrative Rule 8(B)(3).

4. This case involves child support issues. Yes ____ No _X_ *(If yes, supply social security numbers for all family members on a separately attached document filed as confidential information on **light green paper**. Use Form TCM-TR3. 1-4.)*

5. This case involves a protection from abuse order, a workplace violence restraining order, or a no – contact order. Yes ____ No _X_ *(If Yes, the initiating party must provide an address for the purpose of legal service but that address should not be one that exposes the whereabouts of a petitioner.)* The party shall use the following address for purposes of legal service: **N/A**

   _____ Attorney's address

   _____ The Attorney General Confidentiality program address (contact the Attorney General at 1-800-321-1907 or e-mail address is **confidential@atg.in.gov**).

   _____ Another address (provide)

   _____

   This case involves a petition for involuntary commitment. Yes ____ No _X_

6. If Yes above, provide the following regarding the individual subject to the petition for involuntary commitment: **N/A**

7. There are related cases: Yes ____ No _X_ *(If yes, list on continuation page.)*

8. Additional information required by local rule:

   _____

9. There are other party members: Yes ____ No _X_ *(If yes, list on continuation page.)*

10. This form has been served on all other parties and Certificate of Service is attached: Yes _X_ No _____

/s/ Michael Kreppein
Attorney-at-Law
(Attorney information shown above)

CERTIFICATE OF SERVICE

I certify that on December 15, 2021, I electronically filed the foregoing using the Indiana E-Filing System (IEFS). I also certify that on December 15, 2021, the foregoing document was served upon the following persons via IEFS:

Kirk D. Bagrowski
Robert J. Feldt
Eichhorn & Eichhorn, LLP
2929 Carlson Drive, Suite 100
Hammond, IN 46323
kbagrowski@eichhorn-law.com
rfeldt@eichhorn-law.com

/s/ Michael Kreppein
Michael Kreppein (22430-64)

Filed: 12/15/2021 4:00 PM
St. Joseph Circuit Court
St. Joseph County, Indiana

STATE OF INDIANA	)	**IN THE ST. JOSEPH CIRCUIT COURT**
	) **SS:**	
ST. JOSEPH COUNTY	)	
ASPEN SPECIALTY INSURANCE COMPANY, as Subrogee of Trinity Health Corporation, and TRINITY HEALTH CORPORATION,	)	
Plaintiffs,	)	
v.	)	**CAUSE NO. 17C01-2112-CT-000462**
BLACKBAUD, INC.,	)	
Defendant.	)	

CERTIFICATE OF ISSUANCE OF SUMMONS

1. Name of Party or Parties being served:
   Blackbaud, Inc.

2. Date of Mailing:
   December 15, 2021

3. Address of each party being served:
   Blackbaud, Inc., c/o Corporation Service Company, 135 N. Pennsylvania Street, Suite 1610, Indianapolis, IN 46204

4. Tracking Number of each summons:
   7020-0090-0000-7393-0293

Respectfully submitted,

EICHHORN & EICHHORN, LLP

By: /s/ Kirk D. Bagrowski
Kirk D. Bagrowski, #23495-53
Attorney for Trinity Health Corporation

Kirk D. Bagrowski, #23495-53
EICHHORN & EICHHORN, LLP
2929 Carlson Drive, Suite 100
Hammond, Indiana 46323
Telephone: (219) 931-0560
Facsimile: (219) 931-5370

CERTIFICATE OF SERVICE

I, Kirk D. Bagrowski, hereby certify that a copy of the foregoing was served upon:

Blackbaud, Inc.
c/o Corporation Service Company
135 N. Pennsylvania Street, Suite 1610
Indianapolis, IN 46204

by United States First Class Mail (Certified – Return Receipt Requested), postage prepaid, this 15th day of December, 2021.

/s/ Kirk D. Bagrowski
Kirk D. Bagrowski

Filed: 12/15/2021 2:24 PM
Clerk
St. Joseph County, Indiana

STATE OF INDIANA	)	**IN THE ST. JOSEPH CIRCUIT/SUPERIOR COURT**
	) **SS:**	
ST. JOSEPH COUNTY	)	
ASPEN SPECIALTY INSURANCE COMPANY, as Subrogee of Trinity Health Corporation, and TRINITY HEALTH CORPORATION,	)	
Plaintiffs,	)	
v.	)	**CAUSE NO.71C01-2112-CT-000462**
BLACKBAUD, INC.,	)	
Defendant.	)	

COMPLAINT

Plaintiffs, ASPEN SPECIALTY INSURANCE COMPANY ("Aspen"), as subrogee of Trinity Health Corporation, and TRINITY HEALTH CORPORATION ("Trinity Health"), by and through their respective undersigned counsel, and, for causes of action against Defendant BLACKBAUD, INC. ("Defendant" or "Blackbaud"), alleges as follows:

PRELIMINARY STATEMENT

1. This is an action for damages arising out of a February 7, 2020 to May 20, 2020, ransomware incident that infected Blackbaud's computer systems (the "Incident").

2. Blackbaud touts itself as a world leading software company and application service provider ("ASP") that non-profits rely on to secure highly-sensitive information, including personal information from donors and patients.

3. Trinity Health Corporation is an Indiana not-for-profit corporation with a multi-facility health system, including the Saint Joseph Health System that serves St. Joseph County, Indiana and other counties across northern Indiana.

4. On June 17, 2015, Trinity Health contracted with Blackbaud to provide services that consolidated existing databases into one system of records across Trinity Health for enhanced constituent management. A copy of that contract is attached as Complaint Exhibit A.

5. Blackbaud's services included maintaining servers containing Trinity Health's data, including Personally Identifiable Information ("PII") and Protected Health Information ("PHI") (collectively, "Private Information" or "PI").

6. According to the Federal Trade Commission ("FTC"), PII is "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."[1] PHI is deemed private under the Healthcare Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. §§ 1320d, *et seq*.

7. In addition to its contractual obligations to Trinity Health, Blackbaud was required to safeguard Private Information pursuant to federal statutes to ensure that all information it collected and stored was secure.

8. Blackbaud also owed a duty to comply with industry standards in safeguarding Private Information, which – as discussed herein – it did not do. Blackbaud failed to comply with industry and regulatory standards by neglecting to implement security measures to mitigate the risk of unauthorized access, utilizing outdated servers, storing obsolete data, and maintaining unencrypted data fields.

[1] *See* Fed. Trade Comm'n, *Federal Trade Commission Privacy Impact Assessment: Redress Enforcement Database (RED)* at 3, n.3 (June 2019), https://www.ftc.gov/system/files/attachments/privacy-impact-assessments/redress_enforcement_database_red_privacy_impact_assessment_june_2019.pdf.

9. Upon information and belief, on February 7, 2020, a third party was able to readily bypass Blackbaud's substandard security and penetrate Blackbaud's systems and deploy ransomware.

10. Despite Blackbaud's representations that it provided robust cybersecurity services, its security program was woefully inadequate. Blackbaud's unsound, vulnerable systems containing valuable data were an open invitation for a months-long intrusion and exfiltration by cybercriminals

11. Upon information and belief, Blackbaud did not discover the ransomware until on or around May 14, 2020.

12. The Incident resulted in attackers gaining access to Trinity Health's data in Blackbaud's possession regarding its patients' and donors' Private Information.

13. Blackbaud did not inform Trinity Health of the Incident until July 16, 2020.[2]

14. Upon learning of the Incident, Trinity Health, among other things, began notifying impacted patients and donors, set up credit monitoring and an information call center for exposed individuals, and complied with data breach notification laws.

15. Aspen, as Trinity Health's insurer, made payments under its insurance policy (the "Policy") for the costs incurred in responding to the Incident. A redacted copy of the Policy is attached as Exhibit B.

[2] *Trinity Health's Response to the Blackbaud Philanthropy Database Security Incident* (Sept. 14, 2020), https://www.prnewswire.com/news-releases/trinity-healths-response-to-the-blackbaud-philanthropy-database-security-incident-301130466.html.

16. Had Blackbaud maintained a sufficient security program, including properly monitoring its network, security, and communications, it would have discovered the cyberattack sooner or prevented it altogether.

17. Under the Policy Aspen issued to Trinity Health, Trinity Health was responsible to pay the retention and Aspen paid covered amounts in excess of the Policy's retention up to the limit of liability, a combined total of over $2.3 million paid by Trinity Health and Aspen to date.

18. The Policy Aspen issued to Trinity Health grants Aspen the right to pursue third parties, like Blackbaud, for the amounts paid by Trinity Health in satisfaction of the retention and by Aspen under the Policy. Aspen seeks to recover from Blackbaud the damages suffered by Trinity Health and Aspen because of the Incident.

19. Blackbaud's contract with Trinity Health included a provision in which Blackbaud consented to subject matter and personal jurisdiction in state courts in the State of Indiana.

20. Venue is proper in this county because Blackbaud purposely provided ASP services for all of Trinity Health's health-system facilities, including this county, and Trinity Health's injuries are related to Blackbaud's failure to meet such obligations.

21. As a hospital and healthcare provider, Trinity Health must comply with HIPAA and the Health Information Technology for Economic and Clinical Health ("HITECH") Act, including the U.S. Department of Health and Human Services ("HHS") implementing regulations.

22. Under such regulations, "[a] health care provider who transmits any health information in electronic form" is a "Covered Entity." 45 CFR § 160.103, Covered Entity, (3).

23. Under the same regulations, a "Business Associate" includes a corporation who (i) "[o]n behalf of such covered entity or of an organized health care arrangement . . . in which the covered entity participates, . . . creates, receives, maintains, or transmits protected health

information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing;" or (ii) "[p]rovides . . . , legal, actuarial, accounting, consulting, data aggregation . . . , management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person." 45 CFR § 160.103, Business Associate, (1)(i)-(ii).

24. In addition, a "Business Associate" includes "[a] Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information." 45 CFR § 160.103, Business Associate, (3)(i).

25. A 2013 HIPAA amendment made it easier for HIPAA Covered Entities, such as Trinity Health, to identify patients for donations by using software solutions like those offered by Blackbaud to enrich electronic Protected Health Information ("ePHI") to maximize outreach to wealthy patients capable of making a meaningful philanthropic gift to the hospital.

26. ePHI is PHI that is produced, saved, transferred, or received in electronic form. PHI is "[i]ndividually identifiable health information . . . received by a health care provider, health plan, employer or healthcare clearing house [and its Business Associates] . . . [that] [r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual . . . [t]hat identifies the individual; or [w]ith respect to which there is a

reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. §§ 160.103, *et seq*.

27. Blackbaud is a Business Associate, as that term is defined in HIPAA and HITECH, providing functions that involve the use or disclosure of PHI by Covered Entities.

The Master ASP Services Agreement

28. On June 17, 2015, Trinity Health entered a Master ASP Services Agreement (the "Agreement") with Blackbaud for it to provide services.

29. A true, complete, and accurate copy of the Agreement is attached as Exhibit A.

30. Blackbaud represented itself as a provider of ASP services and professional services for nonprofit organizations in addition to the following representations, warranties and obligations:

> 5.1 Services. Vendor represents and warrants to Trinity that it has the skills, expertise and resources to perform, and that it will perform, the Services: . . . (ii) in accordance with industry standards with respect to level of skill, care and diligence . . . .
>
> . . . .
>
> 7.1 Duty of Confidentiality. The Receiving Party shall hold the Confidential Information of Furnishing Party in strictest confidence using the same or greater degree of care it uses with its own most sensitive information (but in no event less than a reasonable degree of care) and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give or disclose such information to third parties or use such information for any purposes whatsoever other than the performance of this Agreement as expressly set forth in this Agreement. The Receiving Patty shall limit access to Confidential Information of the Furnishing Party to only those of its employees, agents and contractors having a need to know in connection with this Agreement or the provision or receipt of the Services, as applicable. The Receiving .Party shall advise all of its employees, agents and contractors who may be exposed to the Confidential Information of the Furnishing Party of' their obligations to keep such information confidential in accordance with this Agreement. The Receiving Party shall be responsible for any breach of confidentiality provisions by such employees agents and contractors. The Receiving Party shall, upon expiration or termination of this Agreement to which. any Confidential, Information relates or otherwise upon demand, at the Furnishing

Party's option, either return to the Furnishing Party or destroy (in each case to the extent permitted by Applicable Law and to the extent commercially practicable) and certify in writing to the Furnishing Party the destruction of any and all Confidential Information of the Furnishing: Party, whether in hard copy or electronic format and whether standalone or included in any other materials or documents, in such Receiving Party's possession, provided, however, that the Receiving Party may retain such limited Confidential Information to the extent required for record retention and audit purposes and subject to the terms of this Agreement.

. . . .

7.5 Security. Vendor shall at all times have in effect a comprehensive information security program that includes reasonable and appropriate technical, administrative and physical security measures aimed at protecting such information from unauthorized access, disclosure, use, alteration or destruction, and that reflects industry-leading practices, including; (i) implementing a documented and auditable change management program; (ii) segregating production and development environments, with non-public data relating to clients limited to the production environment (iii) regular information security training and awareness programs throughout Vendor; (iv) appropriate governance and oversight of information security program-activities; (v). regular independent reviews and audits; (vi) a robust vendor risk management program; (vii) well-documented control processes with corresponding written. procedures; and (viii) comprehensive and regular monitoring of vulnerabilities and security risks. . . . Vendor shall promptly notify Trinity of any security breach

involving Trinity Data, including without limitation any actual or suspected theft, accidental disclosure, or loss of any Trinity Data and/or any unauthorized intrusions into the facilities or secure systems' which contain Confidential Information. In addition, Vendor shall comply with the requirements of all applicable security breach notification statutes.

. . . .

8.6 Meaningful Use. Without limiting Vendor's Support Services obligations, Vendor shall ensure that the ASP Services are compliant, and provided in conformance, with the criteria for meaningful use for an electronic health record, including the privacy and security criteria. Vendor also shall ensure that the ASP Services are compliant with regulations applicable to payment card industry compliance, data breach reporting,. patient rights and federal. and state electronic-records regulations. Vendor shall comply with Trinity's interpretation of state and federal regulation of which Vendor has been informed in writing by Trinity.

. . . .

> 9.4 Limited Data Use. Vendor may not use any Trinity Data, documents, know-how methodologies, software or other materials provided to Vendor for any purpose except to the extent necessary to provide the Services during the Term of this Agreement. Vendor shall not sell, assign, lease, disseminate, or otherwise dispose of Trinity Data or any part thereof to any other person, and Vendor shall not commercially exploit any part of the Trinity Data, even if de-identified.
>
> . . . .
>
> Industry and Security Standards. Vendor shall maintain the security and integrity of Host Computer System and ASP Services consistent with industry standards for comparable services, including maintaining access controls, firewalls, wireless and mobile device and storage Security, virus seaming/protection. software, anti-malware software, encryption of data in transport and storage (including backup data), and network security intrusion protection systems. Vendor shall not take any action that could jeopardize the confidentiality, integrity, availability or security of the System or Trinity Data.[3]
>
> . . . .
>
> Blackbaud adheres to the policies outlined by the PCI Security Standards Council to prevent the retention of sensitive data beyond business requirements.[4]

31. As discussed in more detail below, Blackbaud also agreed to perform ASP services and its other obligations under the Agreement "in a manner that complies with all applicable federal, state and local laws, rules, regulations and standards" and "shall take all measures to promptly remedy any violation(s) of Applicable Law in the performance of the Services and its obligations under [the] Agreement, and shall promptly notify Trinity of any violation(s) thereof."[5]

32. Specifically, Blackbaud represented and agreed to comply with its obligations as a "business associate" under HIPAA, HITECH, and any implementing regulations.[6]

---

[3] Agreement (page 37), ASP Services Exhibit, Section 3.a.

[4] Agreement, Professional Services Statement of Work (Apr. 1, 2015), 3.1 General Assumptions & Responsibilities (page 21).

[5] Agreement, 8.1 General Compliance.

[6] BAA, Section B.

33. Trinity Health entered into the Agreement based on Blackbaud's representations that it would and could comply with its obligations as a "business associate" under HIPAA, HITECH, and any implementing regulations.[7]

The Business Associate Agreement

34. In addition to the Agreement, Blackbaud and Trinity Health entered into a Business Associate Agreement ("BAA"), effective June 17, 2015.[8]

35. A copy of the BAA is attached as Exhibit C.

36. Under the BAA, Blackbaud agreed to comply with its obligations as a "business associate" under HIPAA, HITECH, and any implementing regulations.[9]

37. Blackbaud also agreed "to implement reasonable administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of all PHI." [10]

38. Blackbaud agreed "to implement reasonable electronic security practices for [Trinity Health's] PHI which is transmitted, stored, collected, created, received, maintained, or used in electronic form" and "to encrypt PHI transmitted by [Blackbaud] to [Trinity Health] over a public network"[11]

---

[7] Agreement, Section 4.

[8] Agreement, 7.6 Business Associate Obligations.

[9] BAA, Section B.

[10] BAA, Section G.1.

[11] BAA, Section G.1.

39. Blackbaud was required to report any "actual or suspected privacy incident, breach of security, intrusion or unauthorized use or disclosure of PHI or ePHI" within ten business days.[12]

Blackbaud Breached Its Obligations as a "Business Associate"

40. Covered Entities and their Business Associates, which process PHI and ePHI, must meet strict privacy and security standards propounded by HHS pursuant to HIPAA and HITECH. HHS's Office for Civil Rights ("OCR") is responsible for enforcing the Privacy and Security Rules under HIPAA and HITECH.

41. HIPAA/HITECH mandated security specifications are risk-driven and certain measures must be taken if, after a risk assessment, the specified security measure is determined to be "reasonable and appropriate" in the risk management of the confidentiality, availability, and integrity of ePHI.

42. Blackbaud is a Business Associate, as that term is defined in HIPAA and HITECH, providing functions that involve the use or disclosure of PHI by Covered Entities, like Trinity Health.

43. Blackbaud is a "business associate" subject to HIPAA because it receives, maintains, or transmits its customers' PHI. *Id.* § 160.103. "PHI" includes, in relevant part, individually identifiable health information relating to the provision of health care. *Id.*

44. As a Business Associate, Blackbaud is directly subject to the HIPAA Security Rule.

45. Under the BAA, Blackbaud also agreed to comply with its obligations as a "business associate" under HIPAA, HITECH, and any implementing regulations.[13]

[12] BAA, Section G.2.

[13] BAA, Section B.

46. HIPAA and its implementing regulations, 45 C.F.R. §§ 160, *et seq.*, establish privacy and security standards for certain health organizations and their "business associates." *See id.* § 164.302.

47. For example, HIPAA required Blackbaud to ensure the confidentiality of the electronic PHI it received and maintained by protecting against reasonably anticipated threats to its integrity. *Id.* § 160.306(a). To do so, Blackbaud was required to implement reasonable and appropriate security measures to mitigate the risk of unauthorized access to its customers' electronic personal health information, including by encrypting certain data where appropriate. *See id.* §§ 164.308 (administrative safeguards), 164.312 (technical safeguards).

48. In addition, encryption of ePHI at rest is a commonly implemented security measure for ePHI stored on systems that can be accessed from the internet (including through a client portal).

49. In fact, HHS mandates that organizations encrypt ePHI in motion and at rest whenever it is "reasonable and appropriate" to do so. If encryption is reasonable and appropriate and an organization fails to implement it, it must document its reasons for not doing so in writing. The written documentation should include the factors considered as well as the results of the risk assessment on which the decision was based.

50. Blackbaud was aware of the significant privacy and security obligations of Covered Entities and their Business Associates mandated by HIPAA and HITECH and the Privacy and Security Rules.

51. Blackbaud understood both the value and the risk of using ePHI for fundraising purposes. As stated in one of its white papers, Blackbaud understood:

> [t]he new HIPAA rules offer great opportunity for hospitals and health systems to reach out in a more meaningful way to the individuals and families who have the greatest affinity to them — their patients. **However, with this opportunity comes great responsibility to establish business processes that allow for successful fundraising but also manage and protect the patient data entrusted to you.**[14]

52. Blackbaud breached its obligations as a "business associate" under the BAA by failing to comply with HIPAA, HITECH, and implementing regulations.

Blackbaud's Obligations to Provide Breach Notification as a "Business Associate"

53. As a Business Associate, Blackbaud is directly liable for HIPAA violations for any "failure to comply with the requirements of the Security Rule."

54. As a Business Associate, Blackbaud is also directly liable for HIPAA violations for any "failure to provide breach notification to a covered entity or another business associate."

55. Under the BAA, Blackbaud agreed to comply with its obligations as a "business associate" under HIPAA, HITECH, and any implementing regulations.[15]

56. The HIPAA Breach Notification Rule, 45 C.F.R. § 164.400-414, requires HIPAA Covered Entities and their Business Associates to provide notification following a breach of unsecured PHI. Similar breach notification provisions implemented and enforced by the FTC, apply to vendors of personal health records and their third-party service providers, pursuant to Section 13407 of the HITECH Act.

---

[14] Susan U. McLaughlin, Blackbaud, *HIPAA, PHI, and You* 4 (Feb. 2015), https://www.blackbaud.com/files/resources/downloads/2015/02.15.HIPAA_GratefulPatient.Whitepaper.pdf (emphasis added).

[15] BAA, Section B.

57. A HIPAA breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the PHI. An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
b. The unauthorized person who used the PHI or to whom the disclosure was made;
c. Whether the PHI was actually acquired or viewed; and
d. The extent to which the risk to the PHI has been mitigated.

58. Where there is an unauthorized disclosure or ransomware attack on PHI the Business Associate must document by "thorough and accurate evaluation the evidence acquired and analyzed" to determine whether there is a "low probability of compromise."[16]

59. Under the BAA, Blackbaud represented to Trinity and agreed to comply with the forgoing obligations as a "business associate" under HIPAA, HITECH, and any implementing regulations.[17]

60. Based on the foregoing representations made by Blackbaud, Trinity Health entered into a service agreement for Blackbaud's software and subscription ASP services. [18]

61. Blackbaud breached the BAA by failing to comply with its obligations as a "business associate" under HIPAA, HITECH, and any implementing regulations.

---

[16] Off. for C.R., U.S. Dep't Health Hum. Servs., *FACT SHEET: Ransomware and HIPAA* 6 (2016), https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.

[17] BAA, Section B.

[18] Agreement, Section 4.

Blackbaud's Failure to Maintain Adequate Security

62. Upon information and belief, Blackbaud maintained Trinity Health's data on a shared network, server, and/or software. Despite its own awareness of steady increases of cyberattacks on health care providers over the course of recent years, Blackbaud did not maintain adequate security of Trinity Health's database of Private Information and did not adequately protect it against hackers and cyberattacks.

63. Upon information and belief, Blackbaud maintained Private Information on servers that were obsolete.

64. Upon information and belief, the servers were not on the system patch schedule and were "forgotten machines."

65. Upon information and belief, Blackbaud had planned on upgrading the old servers to new technology.

66. Upon information and belief, the servers that were breached were one of the last environments to be rolled over onto a new platform that Blackbaud was implementing called "Raiser's Edge."

67. Upon information and belief, the older servers were operating multiple applications, and Blackbaud wanted to eventually merge them onto a new, base application on one server.

68. Upon information and belief, upgrading to new technology had been "on a laundry list for a while."

69. Upon information and belief, employees at Blackbaud became increasingly alarmed with Blackbaud's failure to patch old systems, and even eventually emailed executives about the vulnerabilities—receiving a response from one executive: "we're working on it."

70. Upon information and belief, a former information security analyst warned Blackbaud about process vulnerabilities that would subject them to attack—such as using remote desktop access and the vulnerabilities that had been uncovered in security scans.

71. Upon information and belief, the remote desktop access configuration was particularly concerning for a year leading up to the Incident — so much so that s/he or his/her team member would simply "shut down the machines" because they knew the risk was too high to allow them to continue to operate.

72. Upon information and belief, prior to the breach s/he separately advised that CrowdStrike needed to be installed on Blackbaud's machines to capture logs, including the logs that were later erased by the ransomware in this case.

73. Upon information and belief, because Blackbaud elected not to install a program on their servers that would have assisted in the forensic investigation of the Incident, the data that would normally be used in a forensic investigation is limited.

74. Upon information and belief, Blackbaud elected to not have this functionality and, as a result, the data on the Incident is limited.

75. Upon information and belief, the aforementioned analyst's team suggested a year prior to the Incident that the data on Blackbaud's servers needed to be encrypted to reduce vulnerabilities; however, because the servers were so old, the "exact nature of the data was unknown."

76. Upon information and belief, the Incident was the result of Blackbaud's failure not only to properly and adequately determine whether it was susceptible to a data breach but also its negligent and reckless failure to remove old unused and obsolete data containing Private Information or to encrypt such information.

77. Upon information and belief, Blackbaud's retention of this Private Information in unencrypted form on older legacy versions of its programs made public exposure of such data in a cyberattack very likely.

78. Upon information and belief, there was no valid business reason to continue to maintain this information on its systems.

79. The failure was knowing, reckless and, at bare minimum, negligent given the known risks to Blackbaud—particularly given vendor announcements regarding the sunset of certain databases and Blackbaud's failure to move Private Information to newer systems with more robust security features.

80. As a result of Blackbaud's lax data protection standards, cybercriminals obtained access not only to recently-obtained information, but Private Information that remained on backup files for years, if not decades.

Aftermath of Attack

81. Upon information and belief, the ransomware attack that began in February 2020 and continued until May 2020 was twofold: the cybercriminals copied data from the systems and held it for ransom, and upon being discovered, the cybercriminals attempted but allegedly failed to block Blackbaud from accessing its own systems.

82. Upon information and belief, the ransomware attack led to the removal of one or more copies of some or all of the accessed data.

83. Upon information and belief, once removed, the hackers could easily have re-copied the stolen data.

84. Upon information and belief, on May 14, 2020, Blackbaud retained Kudelski Security to "investigate unauthorized activity and scripts detected throughout" Blackbaud's systems.

85. Upon information and belief, Kudelski Security completed its analysis on June 10, 2020, and issued the report ("the Report") on July 14, 2020, [19] two days before Blackbaud contacted Trinity Health to inform it about the Incident.

86. Upon information and belief, the Report shows that Blackbaud did not have a sufficient security program in place to prevent cyberattack and access, and to address the full scope of the Incident.

87. Upon information and belief, the Report highlights the steps it could have taken—but failed to take—to prevent the Incident.

88. In sum, Blackbaud failed to maintain its information on current databases—it failed to heed vendor announcements regarding the sunset of certain databases, leaving client information, including Trinity Health, on older databases that were more vulnerable to cyberattack.

89. Based on the foregoing, Blackbaud breached its contractual obligations to Trinity Health under the Agreement and BAA, and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard Blackbaud's computer systems and the data it maintained. Blackbaud's wrongful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security program to reduce the risk of data breaches and cyberattacks;
b. Failing to adequately protect consumers' Private Information;
c. Failing to properly monitor its own data security programs for existing intrusions;

[19] Kudelski Security, Blackbaud Incident Report (July 14, 2020).

d. Failing to destroy highly confidential personal data information including Social Security numbers on its legacy software which was unnecessarily kept on Blackbaud's systems despite no reasonable or practicable business reason for doing so;
e. Misrepresenting the extent to which Private Information was exposed by the breach;
f. Misrepresenting that Blackbaud would maintain reasonable security measures;
g. Concealing that Blackbaud did not adopt reasonable security measures; and
h. Failing to timely notify Trinity Health of the data breach.

90. As the result of Blackbaud's failure to take certain measures to prevent the attack before it occurred, Blackbaud negligently and wrongfully failed to safeguard Trinity Health's database of Private Information.

The Trinity Health Insurance Policy

91. Trinity Health is an Aspen insured under an Aspen APEX Cyber Insurance Policy attached as Exhibit B.

92. In accordance with the terms of the Policy, Trinity Health paid amounts covered under the retention for Remediation Damages incurred because of the Incident, including, but not limited to, credit monitoring services and call centers, legal counsel, computer systems recovery, and data recovery and data migration services (the "Remediation Damages").

93. Pursuant to the Policy, Aspen paid on behalf of Trinity Health amounts covered under the policy for Remediation Damages necessitated by the Incident.

94. The Policy contains a subrogation clause that states as follows:

> H. Subrogation. If any payment is made under this Policy for Loss or Expense, and there is the ability to recover against any third party, it is agreed that the Insured tenders all its rights of recovery to the Insurer. The Insured also agrees to assist the Insurer in exercising such rights. Any recovery will first be paid to the Insurer toward any incurred subrogation expenses, Loss or Expense, and any remaining amounts will be paid to the Insured for reimbursement of any Retention paid.

95. The subrogation clause grants Aspen the right to recover from Blackbaud the Remediation Damages paid by Trinity Health in satisfaction of the retention and the Remediation Damages paid by Aspen under the Policy.

96. Aspen seeks to recover from Blackbaud the damages suffered by Trinity Health and Aspen because of the Incident.

CAUSES OF ACTION

COUNT I: BREACH OF CONTRACT

97. Plaintiffs re-allege and incorporate each of the foregoing allegations of this Complaint with the same force and effect as if fully set forth herein.

98. The Agreement between Blackbaud and Trinity Health is valid and enforceable.

99. The BAA between Blackbaud and Trinity Health is valid and enforceable.

100. Blackbaud had duties under the Agreement and BAA to, among other things, protect consumers' Private Information, including encrypting Private Information; properly and adequately determine whether it was susceptible to a data breach properly; maintain and monitor its own data security programs for intrusions; and, remove old unused and obsolete data containing Private Information or to encrypt such information.

101. Under the Agreement, Blackbaud agreed not to disseminate Trinity Health's data and not to copy, reproduce or transfer any confidential information.

102. Under the Agreement, Blackbaud agreed to carry and maintain Commercial General Liability insurance and Network liability insurance naming Trinity as an additional insured under its policies. [20]

[20] Agreement, Section 10.

103. Under the BAA, Blackbaud agreed to comply with its obligations as a "business associate" under HIPAA, HITECH, and any implementing regulations.[21]

104. In addition, Blackbaud was required under the BAA to report any "actual or suspected privacy incident, breach of security, intrusion or unauthorized use or disclosure of PHI or ePHI" within ten business days. [22]

105. Blackbaud breached its duties under the Agreement and BAA by, among other things, failing to adequately protect consumers' Private Information; failing to properly and adequately determine whether it was susceptible to a data breach; failing to properly maintain and monitor its own data security programs for intrusions; failing to remove old unused and obsolete data containing Private Information or to encrypt such information; failing to heed vendor announcements regarding the sunset of certain databases, leaving client information on older databases that were more vulnerable to cyberattack; and, failing to name Trinity Health as an additional insured under its policies.

106. Blackbaud also breached its duties by disseminating Trinity Health's data to third parties and permitting them to copy, reproduce and transfer such confidential information.

107. In addition, Blackbaud breached its duties under the BAA by failing to comply with its obligations as a "business associate" under HIPAA, HITECH, and any implementing regulations.[23]

---

[21] BAA, Section B.

[22] BAA, Section G.2.

[23] BAA, Section B.

108. Finally, Blackbaud further breached its duties under the BAA by, among other things, waiting until July 16, 2020 to inform Trinity Health of the Incident despite having to do so under the BAA within ten business days.[24] Blackbaud notified Trinity Health forty-two (42) days after it suspected the Incident was occurring, and twenty-one (21) business days after having full knowledge of the Incident.

109. As a direct and proximate result of Blackbaud's breaches of contract, Trinity Health, and its subrogee Aspen, suffered damages.

110. The damages suffered by Trinity Health, and its subrogee Aspen, include, but are not limited to, paying the Remediation Damages.

111. These damages total an amount no less than $2,317,432.39, and continue to accrue because of the ongoing fallout of the Incident.

COUNT II: NEGLIGENCE

112. Plaintiffs re-allege and incorporate each of the foregoing allegations of this Complaint with the same force and effect as if fully set forth herein.

113. Blackbaud owed duties to Trinity Health under the Agreement and the BAA, federal and state law and regulations, industry standards, and common law to maintain reasonable and appropriate physical, administrative, and technical measures to keep Trinity Health's Private Information confidential and to protect it from unauthorized access and disclosure.

114. Blackbaud breached the duties it owed to Trinity Health by allowing its conduct to fall below the applicable standard of care associated with each of those duties.

[24] BAA, Section G.2.

115. Blackbaud's breach of duties included, but is not limited, failing to adequately protect consumers' Private Information; failing to properly and adequately determine whether it was susceptible to a data breach; failing to properly maintain and monitor its own data security programs for intrusions; failing to remove old unused and obsolete data containing Private Information or to encrypt such information; and, failing to heed vendor announcements regarding the sunset of certain databases, leaving client information on older databases that were more vulnerable to cyberattack.

116. As a direct and proximate result of Blackbaud's negligence, Trinity Health, and its subrogee Aspen, suffered damages.

117. The damages suffered by Trinity Health, and its subrogee Aspen, include, but are not limited to, paying the Remediation Damages.

118. These damages total an amount no less than $2,317,432.39, and continue to accrue because of the ongoing fallout from the Incident.

COUNT III: GROSS NEGLIGENCE

119. Plaintiffs re-allege and incorporate each of the foregoing allegations of this Complaint with the same force and effect as if fully set forth herein.

120. Blackbaud owed duties to Trinity Health under the Agreement and the BAA, federal and state law and regulations, industry standards, and common law to maintain reasonable and appropriate physical, administrative, and technical measures to keep Private Information confidential and to protect it from unauthorized access and disclosure.

121. Blackbaud intentionally failed to perform such duties in reckless disregard of the consequences, because it was previously warned about process vulnerabilities that would subject them to attack and stored Trinity Health's data on obsolete servers.

122. Blackbaud's breach of duties included, but is not limited, failing to adequately protect consumers' Private Information; failing to properly and adequately determine whether it was susceptible to a data breach; failing to properly maintain and monitor its own data security programs for intrusions; failing to remove old unused and obsolete data containing Private Information or to encrypt such information; and, failing to heed vendor announcements regarding the sunset of certain databases, leaving client information on older databases that were more vulnerable to cyberattack.

123. As a direct and proximate result of Blackbaud's gross negligence, Trinity Health, and its subrogee Aspen, suffered damages.

124. The damages suffered by Trinity Health, and its subrogee Aspen, include, but are not limited to, paying the Remediation Damages.

125. These damages total an amount no less than $2,317,432.39, and continue to accrue because of the ongoing fallout of the Incident.

COUNT IV: NEGLIGENT MISREPRESENTATION

126. Plaintiffs re-allege and incorporate each of the foregoing allegations of this Complaint with the same force and effect as if fully set forth herein.

127. Trinity Health entered into discussions with Blackbaud with the expectation that Blackbaud would encrypt and maintain Trinity Health's data on a shared network, server, and/or software because of Blackbaud's reputation as a provider of ASP Services that non-profits rely on to secure highly-sensitive information, including personal information from donors and patients, and so Trinity Health could consolidate existing databases into one system of records across Trinity Health for enhanced constituent management.

128. The Agreement and BAA made clear, among other things, Blackbaud's obligations as a "business associate" under HIPAA, HITECH, and any implementing regulations.[25]

129. Blackbaud made misrepresentations that it could, among other things, comply with such federal law and regulations as well as industry standards to maintain reasonable and appropriate physical, administrative, and technical measures to keep Private Information confidential and to protect it from unauthorized access and disclosure.

130. Blackbaud failed to ascertain whether such representations were accurate.

131. Trinity Health placed confidence in Blackbaud's misrepresentations based on its reputation as purported world leading software company and Trinity Health's reliance on such misrepresentations was an inducement for executing the Agreement and BAA with Blackbaud.

132. As a direct and proximate result of Blackbaud's negligent misrepresentation, Trinity Health, and its subrogee Aspen, suffered damages.

133. The damages suffered by Trinity Health, and its subrogee Aspen, include, but are not limited to, paying the Remediation Damages.

134. These damages total an amount no less than $2,317,432.39, and continue to accrue because of the ongoing fallout of the Incident.

COUNT V: FRAUDULENT MISREPRESENTATION

135. Plaintiffs re-allege and incorporate each of the foregoing allegations of this Complaint with the same force and effect as if fully set forth herein.

136. Trinity Health entered into discussions with Blackbaud with the expectation that Blackbaud would encrypt and maintain Trinity Health's data on a shared network, server, and/or

[25] BAA, Section B.

software because of Blackbaud's reputation as a provider of ASP Services that non-profits rely on to secure highly-sensitive information, including personal information from donors and patients, and so Trinity Health could consolidate existing databases into one system of records across Trinity Health for enhanced constituent management.

137. The Agreement and BAA made clear, among other things, Blackbaud's obligations as a "business associate" under HIPAA, HITECH, and any implementing regulations.[26]

138. Blackbaud made misrepresentations that it could, among other things, comply with such federal law and regulations as well as industry standards to maintain reasonable and appropriate physical, administrative, and technical measures to keep Private Information confidential and to protect it from unauthorized access and disclosure.

139. Blackbaud either knew its representations to Trinity Health were false or recklessly ignored the falseness of its representations, because it was previously warned about process vulnerabilities that would subject them to attack and because Blackbaud stored Trinity Health's data on obsolete servers.

140. Trinity Health relied on Blackbaud's misrepresentations based on its reputation as a purported world leading software company and Trinity Health's reliance on such misrepresentations was an inducement for executing the Agreement and BAA with Blackbaud.

141. As a direct and proximate result of Blackbaud's fraudulent misrepresentation, Trinity Health, and its subrogee Aspen, suffered damages.

142. The damages suffered by Trinity Health, and its subrogee Aspen, include, but are not limited to, paying the Remediation Damages.

[26] BAA, Section B.

143. These damages total an amount no less than $2,317,432.39, and continue to accrue because of the ongoing fallout of the Incident.

COUNT VI: BREACH OF FIDUCIARY DUTY

144. Plaintiffs re-allege and incorporate each of the foregoing allegations of this Complaint with the same force and effect as if fully set forth herein.

145. Blackbaud acted for the benefit of Trinity Health by maintaining Trinity Health's data on Blackbaud's shared network, server, and/or software in a fiduciary capacity as trustee.

146. Trinity Health relied on Blackbaud's promise to maintain reasonable and appropriate physical, administrative, and technical measures to keep Private Information confidential and to protect it from unauthorized access and disclosure.

147. Blackbaud breached its fiduciary duties in acting on behalf of Trinity Health by, among other things, failing to adequately protect consumers' Private Information; failing to properly and adequately determine whether it was susceptible to a data breach; failing to properly maintain and monitor its own data security programs for intrusions; failing to remove old unused and obsolete data containing Private Information or to encrypt such information; and, failing to heed vendor announcements regarding the sunset of certain databases, leaving client information on older databases that were more vulnerable to cyberattack.

148. As a direct and proximate result of Blackbaud's breach of fiduciary duty, Trinity Health, and its subrogee Aspen, suffered damages.

149. The damages suffered by Trinity Health, and its subrogee Aspen, include, but are not limited to, paying the Remediation Damages.

150. These damages total an amount no less than $2,317,432.39, and continue to accrue because of the ongoing fallout of the Incident.

WHEREFORE, the Plaintiffs pray for any and all just and appropriate relief for the breach of contract, negligence claims, and breach of fiduciary duty, including but not limited to any and all compensatory and consequential damages, for any and all punitive damages, for any and all costs of suit and attorney fees, and for any and all relief that may be just and appropriate, including but not limited to, pre- and post-judgment interest, fees and costs.

Respectfully submitted,

/s/Michael A. Kreppein
Michael A. Kreppein, 22430-64
WILSON, ELSER, MOSKOWITZ,
EDELMAN & DICKER LLP
233 E. 84th Drive – Park Tower, Suite 201
Merrillville, IN 46410
Telephone: (219) 525-0560
Michael.Kreppein@wilsonelser.com

Attorney for Plaintiff
ASPEN SPECIALTY INSURANCE COMPANY

/s/ Kirk D. Bagrowski
Kirk D. Bagrowski, 23495-53
Eichhorn & Eichhorn, LLP
2929 Carlson Drive, Suite 100
Hammond, IN 46323
(219) 931-0560
kbagrowski@eichhorn-law.com

/s/ Robert J. Feldt
Robert J. Feldt, 16311-45
Eichhorn & Eichhorn, LLP
2929 Carlson Drive, Suite 100
Hammond, IN 46323
(219) 931-0560
rfeldt@eichhorn-law.com

Attorneys for Plaintiff
TRINITY HEALTH CORPORATION

71G01-2112-CT-000462
St. Joseph Circuit Court
Filed 12/15/2021 2:24 PM
Clerk
St. Joseph County, Indiana

Execution Version

MASTER ASP SERVICES AGREEMENT

This Master ASP Services Agreement is made and entered into as of this 17th **day of June 2015,** ("Effective Date") by and between **Trinity Health Corporation,** an Indiana non-profit corporation with an address of 20555 Victor Parkway, Livonia, Michigan 48152 ("Trinity"), and Blackbaud, Inc., a Delaware corporation having offices at 2000 Daniel Island Drive Charleston, SC 29492 ("Vendor").

BACKGROUND

WHEREAS, Vendor is a provider of ASP Services and Professional Services for nonprofit organizations;

WHEREAS, Trinity and Vendor desire to enter into this Master ASP Service Agreement in order to agree upon the prices, terms and conditions upon which Trinity may purchase the services described herein from Vendor;

NOW THEREFORE, in consideration of the mutual promises set forth below, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties hereto, intending to be legally bound, agree as follows:

1. DEFINITIONS

"Affiliate" shall mean the "system office" of Trinity and each of the "Regional Health Ministries", "Mission Health Ministries", managed hospitals and hospital joint ventures and each of their respective associated foundations (if applicable), in each case, which are either directly or indirectly owned or controlled by Trinity. "Control" as used in this Agreement means the ability to direct the affairs of an entity, whether through ownership of at least a majority interest in an entity, possession of a majority of the votes on the governance board of an entity, reserved powers or by contract, including a management, joint operating or other substantial agreement.

"Agreement" shall mean and refer to the terms of this Master ASP Services Agreement, as well as any Orders, Exhibits, attachments, and other documents referenced herein.

"Authorized User" means a person designated by Trinity or a Trinity Affiliate to use the Blackbaud Solutions for or on behalf of Trinity and or a Trinity Affiliate consistent with the licenses set forth in the applicable Order Form.

"Blackbaud Solutions" shall mean any Software, subscriptions and Services including application services and payments services, support and maintenance ("*Maintenance*"), and other professional, consulting or training services provided by Vendor and detailed in the applicable Order Form.

"Chronic Service Issue" shall mean Vendor's failure in (i) three (3) consecutive months or (ii) any five (5) months in any twelve (12) month rolling period, to provide 99.5% or greater "Availability" (as defined in the Hosting and Service Level Exhibit) in such months against the production environment.

Exhibit A

"Confidential Information" shall mean all proprietary, secret or other information or data in any format (spoken, electronic or hardcopy) belonging to, concerning or in the possession or control of a Party or an Affiliate (the "*Furnishing Party*") that is furnished, disclosed or otherwise made available to the other Party (the "*Receiving Party*") (or entities or persons acting on the other Party's behalf) in connection with this Agreement and which is either marked or identified in writing as confidential, proprietary, secret or with another designation sufficient to give notice of its sensitive nature, or is of a type that a reasonable person would recognize it to be commercially sensitive. In the case of Affiliate, "Confidential Information" includes any non-public information to which Vendor Personnel have access in Affiliate locations or Affiliate's information systems.

"Deliverables" shall mean any work product (i) specifically identified as a Deliverable in this Agreement or the applicable Order, or (ii) provided by Vendor to Trinity pursuant to this Agreement.

"Documentation" shall mean the applicable manuals and documentation that Vendor generally provides or makes available for Vendor's Software, subscriptions, maintenance, and Services.

"Enhancement" shall mean, in respect of the Software, any release, update, or version, including those that operate on a different or new equipment platform or version of operating system or database software, and any other improvement, modification, upgrade, update, fix or addition to the Software, irrespective of how designated, classified or marketed. Re-named and/or re-packaged Software, and "next-generation" versions or re-releases of the Software, shall be treated as an Enhancement for purposes of the Agreement.

"Host Computer System" or "System" shall mean the Software, hardware and related infrastructure maintained by Vendor in order to enable Vendor to provide ASP Services to its customers, including Trinity.

"Intellectual Property Rights" means all (i) patents, patent disclosures and inventions (whether patentable or not), (ii) trademarks, service marks, trade dress, trade names, logos, corporate names and domain names, together with all of the goodwill associated therewith, (iii) copyrights and copyrightable works (including computer programs), and rights in data and databases, (iv) trade secrets, know-how and other confidential information, and (v) all other intellectual property rights, in each case whether registered or unregistered and including all applications for, and renewals or extensions of, such rights, and all similar or equivalent rights or forms of protection in any part of the world.

"Order" shall mean the agreement entered into by Trinity and Vendor using the form set forth on the attached Order Form Exhibit. Each Order shall include: (a) a description of the product and/or Services to be provided, (b) the charges for such product and/or Services (based on the fees set forth in the attached Services Exhibit, as applicable), and (c) any other mutually agreed terms.

"Party" shall mean Vendor and Trinity. Vendor and Trinity are each individually referred to herein as a "Party" and sometimes collectively referred to hereinafter as the "Parties."

"Performance Credit" shall mean a monetary credit to which Trinity is entitled as a result of a default or otherwise for Vendor's failure to meet the service level requirements ("SLAs") as set forth in the attached Hosting and Service Level Exhibit.

"Services" shall mean all ASP Services (including Software and Support Services) and Professional Services and any Deliverables provided by Vendor to Trinity and its Affiliates as set forth in this Agreement and as

further described on the attached Services Exhibit and the applicable Order. The Services Exhibit describes the Services that are available to be purchased by Trinity and its Affiliates from Vendor as of the Effective Date and the corresponding fees for such Services.

"Scope-of-Use Limitations" shall mean any usage limitations that apply to Software licensed under the Agreement, each of which, if applicable, shall be specified in the applicable Order.

"Software" shall mean any software provided by Vendor under this Agreement.

"Trinity Data" shall mean any and all information provided by Trinity or any Affiliate to Vendor, including any Confidential Information.

"Vendor Personnel" shall mean Vendor's employees, agents and subcontractors or other persons or entities which provide any items or services on behalf of, or at the direction of, Vendor under this Agreement.

2. PARTICIPATION BY TRINITY AFFILIATES

2.1 Scope of Participation. Vendor agrees that, subject to the licenses set forth in the applicable Order Form (e.g. concurrent user licenses, etc.), employees and agents of Trinity and Trinity's Affiliates shall have the right to use or access the Blackbaud Solutions purchased by Trinity pursuant to the Agreement.

2.2 Orders. Unless otherwise directed in writing by Trinity, all Orders will be executed by Trinity and Vendor. No Order shall be effective unless signed by a duly authorized representative of Trinity and Vendor.

2.3 Terms. The terms and conditions of this Agreement will apply to all Orders and govern all purchases of Blackbaud Solutions by Trinity.

2.4 Transfer of Services.

2.4.1 The purchase by Trinity of the Blackbaud Solutions described in the Order Form dated as of the Effective Date includes, among other things, Services relating to the consolidation of certain databases of Trinity Affiliates into a single, consolidated CRM database. A portion of such Trinity Affiliates use, pursuant to existing agreement(s) with Vendor, Blackbaud Solutions (Raisers Edge) to manage their individual databases. The parties agree that as the consolidation of such individual Affiliate databases into the CRM database is performed, the existing agreement(s) between such Affiliates and Vendor will be terminated.

2.4.2 If, following the Effective Date, an existing Vendor customer becomes a Trinity Affiliate and Trinity notifies Vendor in writing of the customer's Trinity Affiliate status, then the Parties shall terminate the existing agreement(s) between Vendor and such new Trinity Affiliate and incorporate such new Trinity Affiliate within the scope of the Agreement by executing an Order (and such previously licensed and/or purchased services shall be subject in all respects to the terms of the Agreement as though originally licensed and/or provided herein).

2.4.3 If Trinity directly or indirectly divests, closes or otherwise ceases to own or Control an Affiliate that is then receiving Services under this Agreement (each, a "Divested Entity"), Vendor agrees

that Trinity shall have the right to permit a Divested Entity to continue receiving the Services for up to thirty-six (36) months following the effective date of the divestiture. If any Services are subject to Scope-of-Use Limitations, Trinity shall have the right if it discontinues use of such Services, to either: (a) "bank" the licenses that were then being used by such Divested Entity for future use by a different Trinity Affiliate, or (b) transfer the licenses that were then being used by such Divested Entity to a different Trinity Affiliate.

2.5 Non-Exclusive Agreement. This Agreement does not confer on Vendor the right to be the exclusive provider of any type of services to Trinity or its Affiliates. The Parties acknowledge and agree that the execution of this Agreement is not a guarantee of future work (other than future work set forth in an Order From executed by the Parties) or of any minimum payment or volume commitment.

3. PRICING AND PAYMENT

3.1 Pricing. All fees payable to Vendor during the term of this Agreement shall be determined based on the rates for the Blackbaud Solutions set forth on the Services Exhibit, which (other than change orders implemented during the project) represent the totality of charges under this Agreement. Unless otherwise set forth in an applicable Order Form executed by the Parties, the Parties agree that fees for the Services shall not commence until the date of Acceptance of the Services. Vendor shall not be entitled to invoice, nor shall Trinity be obligated to pay, any charges for which the rates therefor are not expressly stated in the Services Exhibit or in an applicable Order Form, including without limitation, miscellaneous fees, administrative costs, taxes or government surcharges. When requested by Trinity, the Parties shall update the Services Exhibit to reflect: (a) the addition of any additional Services Trinity has decided to purchase from Vendor following the Effective Date, as well as the fees for such services, which fees shall be negotiated by the Parties at such time, and (b) the deletion of any Services that Trinity has decided to no longer purchase from Vendor following the Effective Date.

3.2 Price Protection. Vendor agrees to hold firm the prices offered in the Services Exhibit for the entire Term of this Agreement. The pricing in each Order will reflect these rates.

3.3 Payment Schedule and Invoicing. Payment for the Services under this Agreement is due within forty-five (45) days of Trinity's receipt of Vendor's complete invoice and all payments must be made without deduction or offset, except for those amounts for which there is a good faith dispute. All payments are non-refundable except as otherwise provided in this Agreement. All invoices shall be in U.S. dollars and must include the applicable purchase order number to be processed for payment. Invoices received without the appropriate purchase order number shall not be considered valid for payment. Vendor shall review all invoices for accuracy prior to submitting them to Trinity and shall maintain complete and accurate records, in a form in accordance with generally accepted accounting practices, to substantiate any amounts invoiced by Vendor.

3.4 Invoice Dispute. All invoices shall be deemed final and binding unless Trinity notifies Vendor in writing of any alleged discrepancies no later than forty-five (45) days from the date of such invoice. If Trinity provides such notice, Trinity may withhold payment on any invoiced amounts reasonably disputed in good faith under this Agreement; provided, however, that Trinity shall (i) provide a detailed written explanation to support the withholding of any disputed amounts; and (ii) timely pay any undisputed amounts on the invoice. Such nonpayment by Trinity shall not constitute a breach of Trinity's obligations of payment and the Parties shall work together in good faith to resolve the dispute

in a timely manner. Vendor shall continue performing its obligations in accordance with this Agreement notwithstanding any such dispute or actual or alleged nonpayment that is the subject of the dispute, pending its resolution.

3.5 Expenses. All travel expenses incurred by Vendor will be mutually agreed to by the Parties' respective project management teams prior to travel expenses being incurred. Vendor shall comply with the Travel Policy attached as the Travel Policy Exhibit. Trinity shall not be responsible to reimburse Vendor for any travel expense which fails to comply with such Travel Policy.

3.6 Taxes. Trinity and its Affiliates are tax-exempt entities and shall provide Vendor with reasonable evidence of exemption from taxes. If a purchase is exempt from any otherwise applicable sales, use, privilege, excise or other taxes, Vendor shall not charge Trinity such tax. To the extent Vendor is required to collect a tax from a tax-exempt purchaser under Applicable Law, Vendor shall separately state the amount of taxes due on its invoices to Trinity and identify the governmental authority whose tax is being charged. Vendor shall be responsible for all other taxes, including taxes based upon Vendor's own income, medical device excise taxes and property taxes.

4. SERVICE REQUIREMENTS

4.1 Software.

4.1.1 Software License Grant. In respect of Software specified in the applicable Order, Vendor grants to Trinity, and Trinity accepts, an irrevocable, nontransferable, nonassignable, nonsublicensable, nonexclusive, and perpetual license to use one (1) copy of the Software in machine readable object code form only ("License"). The License includes the right to use the applicable manuals and documentation that Vendor generally provides or makes available for Blackbaud Solutions ("Documentation") solely for the furtherance of Trinity's internal business purposes. The License extends to the computer program delivered by Vendor and Enhancements provided by Vendor pursuant to Trinity's continued enrollment in Maintenance and, where applicable, applications created by or on behalf of Trinity utilizing the Application Programming Interface, Software Development Kit, or Visual Basic for Application contained in the Software ("Blackbaud Tools"). Trinity may only install and use the Software (i) in a manner that ensures that Trinity's simultaneous use of and access to the Software will be limited as set forth in the applicable Order Form. Unless otherwise expressly set forth in an Order Form, Trinity shall not share Licenses with any persons that are not Affiliates without the express written agreement of Vendor and Trinity's payment of additional License fees.

4.1.2 Software License Termination. Unless terminated pursuant to this Section 4.1.2, the License is effective in perpetuity. Trinity may terminate a License at any time by providing written notice to Vendor. Vendor shall have the right to terminate a License by providing written notice to Trinity (i) upon Trinity's failure to pay when due any undisputed invoiced amount(s) applicable to such License, provided that Vendor has given Trinity at least fifteen (15) days prior written notice of Vendor's intention to terminate the License and Trinity fails to pay the undisputed invoiced amount(s) during that fifteen (15) day period, (ii) upon Trinity's failure to cure a material default applicable to such License, pursuant to Section 6.2.1, or (iii) if Vendor is unable, using commercially reasonable efforts, to obtain the right for Trinity to continue using the Software if the Software becomes the subject of an infringement claim for which Vendor is indemnifying Trinity pursuant to Section 10.4 below. Within

thirty (30) days after the effective date of termination of a License Trinity shall return all copies of the Software to Vendor or certify in writing to Vendor that it has destroyed or erased all copies of the Software.

4.1.3 Ownership of Software. No title or ownership of Intellectual Property Rights to the Software or Documentation are transferred to Trinity under the Agreement; all such rights are retained by Vendor. Except to the extent permitted under the Agreement, Trinity shall not: (a) modify, copy or create any derivative works of, the Software or the Documentation, (b) license, sublicense, sell, resell, lease, transfer, assign, distribute, time share, offer in a service bureau or otherwise make the Software or Documentation available to a third party, or (c) reverse engineer or decompile any portion of the Software except as necessary to create interoperate computer programs.

4.1.4 Documentation of Software. On or about the date on which Software is provided or otherwise made available to Trinity, Vendor shall provide to Trinity, or make available for download by Trinity, Documentation that is reasonably detailed and complete and that accurately describes the functional and operational characteristics of such Software. In addition, Vendor shall provide to Trinity, or make available for download by Trinity, updated versions of all such Documentation as soon as reasonably practical following its release by Vendor, but in no event later than ten (10) days following delivery of any Enhancement to Trinity. Updated Documentation will be at least as detailed as the Documentation provided or made available to Trinity with any initial Software delivery.

4.2 Subscription.

4.2.1 Subscription Access. In respect of the Subscription specified in the applicable Order Form, Vendor grants to Trinity, and Trinity accepts, a nonassignable, nontransferable, nonsublicensable, and nonexclusive right to access the Subscription and use the Subscription and Documentation solely for the furtherance of Trinity's internal business purposes during the Subscription term set forth on the Order Form. Subscriptions will not be provided to Trinity on any form of media and will not be installed on any servers or other computer equipment owned or otherwise controlled by Trinity. During the Subscription term Vendor shall provide Trinity with secure access via the Host Computer System to the latest supported version of the Subscription, to be accessed and used by Trinity through the use of the Internet. Vendor shall provide Trinity with administrator rights permitting secure administrator access and allowing the administrator to create other users to access the Subscription. Trinity agrees that to the extent a Subscription is specified in an Order From, Trinity has elected to access the Vendor offering through a Subscription and that this Agreement confers no right to convert the Subscription to a License. Trinity's use of the Subscription is subject to the scope of the use provisions above and unless otherwise expressly set forth in an Order Form, Trinity shall not share Subscriptions with any persons that are not Authorized Users of Trinity or Trinity Affiliates without the express written agreement of Vendor and Trinity's payment of additional Subscription fees, if applicable.

4.2.2 Subscriptions and Maintenance Renewals and Cancellations. Unless cancelled in accordance with this section, Subscriptions and Maintenance shall renew for consecutive one (1) year terms following the initial term set forth on the Order Form. Renewal fees for Subscriptions and Maintenance are subject to an adjustment, such adjustment to be included in the renewal notice. Trinity may cancel a Subscription or Maintenance by providing written notice to Vendor at least forty-five (45) days prior to the start of the renewal term. No credit or refunds will be given for partial Subscription or Maintenance periods except if this Agreement is terminated pursuant to Section 6.2 (Termination for Cause) or Section 10.4

(Intellectual Property Indemnification). Cancellations will become effective as of the final day of the then-current term. Reinstatement of a lapsed Maintenance requires full payment of fees that would have been due from the expiration of the last active term through the reinstatement date. Reinstatement of a lapsed Subscription requires full payment of Vendor's then-current Subscription fees.

4.3 ASP Services. The scope of Services will be deemed to include the ASP Services and the requirements set forth in the attached ASP Services Exhibit.

4.3.1 Testing Process. Certain Services as agreed to by the Parties and specified in the applicable Statement of Work shall be subject to testing in accordance with the terms and conditions set forth in the attached Testing and Acceptance Exhibit (the "Testing Process"). Trinity reserves the right to perform reasonable testing prior to Acceptance by Trinity on any Software, Subscription or other Deliverable furnished pursuant to this Agreement to validate that it substantially conforms to the Documentation and any other criteria specified in this Agreement or in the applicable Statement of Work.

4.3.2 Support Services. Vendor shall support and maintain the Software and Subscriptions in accordance with the terms set forth in the attached Support Services Exhibit (such Services, the "Support Services").

4.4 System Requirements. Certain Blackbaud Solutions may only be used or accessed from Trinity's computer systems that meet the Vendor system requirements published at https://www.blackbaud.com/systemrequirements, which Trinity acknowledges it has reviewed.

4.5 Suspension; Acceptable Use Policy. Vendor may suspend Trinity's use of or access to the applicable Blackbaud Solution(s) upon written notice to Trinity (i) in response to Trinity's failure to pay when due any undisputed invoiced amount(s) pursuant to this Agreement, provided that Vendor has given Trinity at least fifteen (15) days prior written notice of Vendor's intention to suspend the Blackbaud Solution and Trinity fails to pay the undisputed invoiced amount(s) during that fifteen (15) day period, or (ii) in response to a violation by Trinity of the acceptable use policy posted at: http://internet.blackbaud.com/eua/aupolicy ("AUP"); provided that Vendor shall use reasonable efforts to notify Trinity of its intention to suspend the Blackbaud Solution and provide Trinity with an opportunity to cure before taking any such action, if practicable and if permitted by law. Vendor will lift any payment-related suspension promptly following Trinity's payment of the undisputed invoice on which the suspension is based. When exercising its right to suspend a Blackbaud Solution for a breach of the AUP, Vendor will respond in a manner proportionate to the severity of the violation (e.g., when a single user has breached the AUP, by suspending Subscription access to the user rather than suspending all users or Blackbaud Solutions). With respect to any suspension, Vendor and Trinity agree to work together in good faith to address the violation in a reasonable manner, to prevent similar violations in the future, and to reinstate the suspended Blackbaud Solution as quickly as possible.

4.6 Trinity Control. Trinity shall be solely responsible for administering and monitoring the use of login IDs and passwords by its administrators and users. Upon the termination of employment of any such Trinity administrator or user Trinity will immediately terminate access by the login ID and password of that individual to Blackbaud Solutions. Vendor is not responsible for any damages resulting from Trinity's failure to manage the confidentiality of its login ID and passwords. Vendor will not solicit any contributions for or on behalf of Trinity, and will not employ or procure any person to do so.

4.7 Prohibited Uses. Trinity shall not modify, rent, sublease, sublicense, assign, use as a service bureau, copy, lend, adapt, translate, sell, distribute, derive works from, decompile, or reverse engineer Blackbaud Solutions, except as explicitly permitted hereunder. Unless otherwise expressly set forth in an Order Form, Blackbaud Solutions shall be used solely by Trinity and its Affiliates, and not (by implication or otherwise) by any other person. Trinity shall not: (a) knowingly send or store material containing software viruses, worms, Trojan horses or other harmful computer code, files, scripts, agents or programs in, to or from Blackbaud Solutions; (b) interfere with or disrupt the integrity or performance of Blackbaud Solutions, or the data contained therein; (c) use Blackbaud Solutions in a manner inconsistent with applicable Documentation; or (d) attempt to gain unauthorized access to Blackbaud Solutions or related systems or networks.

4.8 Professional Services. Each Order that involves Vendor's provision of Professional Services shall include the following documents, if and to the extent requested by Trinity: (i) a Statement of Work that describes the Professional Services to be provided, including the Parties' respective roles and responsibilities; and (ii) an integrated Project Schedule, each of which shall be created jointly by the parties and attached to the Order prior to the Order being signed by Trinity.

4.8.1 Each Project Schedule must: (a) be developed in a project format mutually agreed to by the Parties; (b) reflect all project activities, tasks and subtasks to be performed by Vendor, Trinity and any third parties, and the estimated work effort, in hours, for each such activity, task and subtask; (c) reflect all dependencies; (d) specify any critical milestones, activities and/or projects; and (e) set forth commencement and completion dates for each project activity, task and subtask. Subject to Trinity's review and approval, Vendor shall be responsible for updating each Project Schedule from time to time as necessary to reflect any mutually agreed changes and reporting on the overall project status.

4.8.2 On a mutually agreed upon frequency during the pendency of any project and otherwise promptly following Trinity's request from time to time, representatives of the Parties shall meet by teleconference, video conference or in person to discuss the status of any Project Schedules, including any difficulties or issues that may exist and any proposed changes to any date or other item set forth in any Project Schedule. Vendor shall provide to Trinity a written report of the status of such ongoing projects prior to the status meetings. If applicable, Vendor shall identify any problems, difficulties or other circumstances that Vendor claims have or will impact its ability to meet any critical milestone or other date set forth in a Project Schedule.

4.8.3 Changes to any Statement of Work will require an amendment to the applicable Order pursuant to a Change Order. If either Party believes that a change in the Professional Services or a project is necessary or desirable, such Party shall submit a written change request to the other party. The change request will specify in detail: (i) the requested changes in the Professional Services; (ii) the reason for the requested changes; and (iii) the cost or savings associated with the requested changes. Upon receipt of a change request, the Parties shall engage in good faith negotiations in an effort to reach agreement on the terms of a Change Order, if necessary. Each Party shall bear its own costs and expenses in connection with preparing, reviewing and responding to any change requests.

4.9 Interfaces. Vendor acknowledges that Trinity is working with a number of third parties to develop, maintain and support various ancillary systems and departments and that it may be necessary to use one

or more interfaces between such ancillary systems and departments and the ASP Services. Vendor agrees that it will cooperate and work with Trinity and such third parties to use Vendor's standard interfaces, or to develop custom interfaces (each, a "Custom Interface") using as many industry-standard protocols as possible, in order to allow information to pass from the ancillary systems and departments to the ASP Services and from the ASP Services to the ancillary systems and departments. Vendor acknowledges and agrees that each interface must be deployed in a manner that ensures data is securely transmitted and the identification of communicating systems is verified.

4.9.1 If Trinity requires a Custom Interface, such Custom Interface will be treated as a Deliverable, and Vendor shall develop such Custom Interface in accordance with the terms and conditions set forth in the applicable Order. Unless the parties expressly agree otherwise in the applicable Order, each standard interface and each Custom Interface shall be included within the scope of Vendor's Support Services obligations.

4.9.2 Interface Documentation and Interface Changes. Prior to Acceptance for the applicable ASP Services, Vendor shall provide to Trinity Documentation for each Vendor standard interface and each Custom Interface (such Documentation for each such interface, "Interface Documentation"). Trinity's receipt of such Interface Documentation shall be a condition of Acceptance for the applicable ASP Services. After Services Acceptance for the applicable ASP Services, Vendor shall provide Interface Documentation for Enhancements to Vendor's standard interfaces and Custom Interfaces in accordance with its Support Services obligations.

4.10 Deliverables. Vendor shall complete and deliver all Deliverables in accordance with the specifications and the terms and conditions of this Agreement. Vendor shall review all Deliverables to ensure that such Deliverables comply with the applicable requirements and specifications prior to delivering them to Trinity for review and approval. Each Deliverable provided by Vendor shall be in a form, format, and in such detail as is required or necessary to cause it to conform to the applicable specifications, including any Acceptance criteria that may be specified in the applicable Order. Prior to finalizing any Deliverable, Vendor will provide Trinity's designated personnel with a 'DRAFT' copy for review and comment. Trinity shall have a minimum ten (10) business days after receipt of the DRAFT to evaluate the Deliverable and request corrections or clarifications as appropriate. Promptly following its receipt of a final Deliverable, Trinity shall review the Deliverable for purposes of determining whether it conforms to the specifications. If Trinity determines that the Deliverable conforms to the specifications, Trinity promptly shall so notify Vendor. If Trinity determines that the Deliverable does not conform to the specifications, Trinity promptly shall notify Vendor of the deficiencies, and Vendor promptly thereafter will modify the Deliverable and resubmit it to Trinity for its review (and Trinity promptly shall re-review such modified Deliverable). Without limiting any other rights and remedies that may be available to Trinity, and without extending or otherwise affecting any time-based deadline, the process described herein will repeat until the Deliverable conforms to the specifications and is accepted by Trinity, and Vendor shall perform its obligations relating thereto without additional cost or expense to Trinity; provided, however, that any new requirements that are in addition to the original specifications will require a Change Order. Trinity shall be entitled to rely on any information or data utilized or provided by Vendor in providing the Deliverables, including benchmark or reference data, which shall be current and reliable.

4.11 Service Level Requirements. The attached Hosting and Service Level Exhibit sets forth the various service levels and performance targets applicable to the Services (the "SLAs"), the framework for

Performance Credits for service level failures, and the mechanisms and processes to be used to monitor and assess Vendor's performance of the Services performed hereunder generally. Vendor shall pay to Trinity Performance Credits with respect to any SLA failure in recognition of the diminished value of the Services resulting from Vendor's failure to meet the SLA requirements, and not as damages or a penalty. Vendor's obligation to pay Performance Credits to Trinity, and Trinity's receipt of Performance Credits, shall not be deemed or construed to be a sole and exclusive remedy and shall not limit any rights or remedies Trinity may have under this Agreement or at law, in equity, or otherwise.

4.12 Duty to Communicate Changes to Blackbaud Solutions. Vendor shall provide reasonable notice and/or communication to Trinity in respect of updates or changes to the relevant Blackbaud Solutions in accordance with Vendor's established procedures for such notices or communications and consistent with the Support Services Exhibit which sets forth Vendor's obligations to communicate information about "Covered Software," "Upgrades," and "Planned Obsolescence" (as such terms are defined in the Support Services Exhibit). Vendor's current established procedures for such notices and communications include product specific information on the BlackbaudKnowHow page (http://www.blackbaudknowhow.com/), release and patch information and a release guide on the Downloads page of www.blackbaud.com, information about upcoming and past releases on the Knowledgebase of www.blackbaud.com, and with respect to Blackbaud CRM, quarterly online roadmap meetings to review features and upcoming releases.

4.13 Vendor Personnel. All Vendor Personnel assigned to perform Services under this Agreement shall have appropriate experience and educational credentials and suitable training and skills in the areas for which they are responsible and the tasks to which they will be assigned.

4.13.1 Vendor shall comply with, and ensure that all Vendor Personnel comply with, all rules, regulations and policies of Trinity that are communicated to Vendor, including, as applicable, but without limitation, security procedures concerning systems and data and remote access thereto, building security procedures, credentialing and other applicable procedures. Vendor Personnel shall conduct themselves in a professional and businesslike manner at all times.

4.13.2 For any Services that require access to a Trinity location, Vendor shall provide Trinity with written space requests and coordinate with Trinity to gain approval and access to such location. Vendor shall prepare any necessary forms as directed by Trinity for on-site Vendor Personnel (e.g., submitting requests for badges for Vendor Personnel). Vendor shall at all times keep Trinity locations in good order, not commit or permit waste or damage to them or use them for any unlawful purpose or act.

4.13.3 Vendor shall conduct a background check in connection with its employment-screening processes on all Vendor Personnel who have access to Trinity's systems, facilities or Confidential Information. Such background check shall include, subject to Applicable Laws, a regular background check on the individual's conviction record, drug testing and an employment history verification.

4.13.4 During the currency of a project, Trinity shall have the right to review the performance of Vendor Personnel with Vendor management, and to request removal of Vendor Personnel in the event of significant performance issues provided that the Parties agree to review such a request in good faith before removal is actually made. Vendor requires written notification from Trinity

requesting that Vendor Personnel be removed. In such cases, the costs of transition/knowledge transfer between Vendor Personnel will be performed at no cost to Trinity. Likewise, Vendor shall have the right to review the performance of Trinity personnel with Trinity management and request removal of such Trinity personnel in the event of significant performance issues, provided that the Parties agree to review such a request in good faith before removal is actually made. Trinity requires written notification from Vendor requesting that Trinity personnel be removed.

4.13.5 Notwithstanding any contrary provision in Section 4.12.4, Trinity shall have the right to require the immediate removal and replacement of any individual Vendor Personnel for any misconduct, illegality, or material violation of Trinity's Corporate Compliance Program (as described in Section 8.4 and including such program's Standards of Conduct and Vendor Code of Conduct) upon written notice to Vendor. Vendor is solely responsible for all costs related to the removal or replacement of Vendor Personnel pursuant to this Section 4.12.5. Vendor remains solely responsible for all employer-type matters and liabilities, including those matters associated with recruiting, hiring, employment, compensation, benefits, insurance, promotion, discipline, discharge and work environment of each Vendor Personnel.

4.13.6 Vendor shall be responsible for performing the Services and its obligations hereunder notwithstanding the turnover of any Vendor Personnel, and any attrition and turnover shall under no circumstances relieve Vendor of any of its obligations set forth in this Agreement.

4.13.7 Trinity and Vendor may designate certain employees of Vendor as Vendor Key Personnel. Vendor Key Personnel shall include, at a minimum, those individuals identified in the Order or Statement of Work as Key Personnel and the Vendor Relationship Manager. Vendor Key Personnel must be reasonably available by phone or email as required by Trinity to address any issues or problems that arise during the performance of the Services. Vendor will strive to minimize turnover of Vendor Key Personnel and any reassignment or replacement of Vendor Key Personnel by Vendor will be made only with prior consultation with Trinity. Any dispute related to the provisions of this Section 4.12.7 will be resolved in accordance with the procedures set forth in the Project Charter described in the applicable Statement of Work.

4.13.8 Vendor shall ensure that Vendor Personnel are familiar with the performance standards of this Agreement and all applicable health care standards and regulations, including, without limitation, HIPAA. Vendor and Vendor Personnel shall immediately report any compliance concerns to Trinity.

4.14 Subcontractors. With Trinity's approval for each instance, Vendor may use subcontractors in its performance of this Agreement. Any subcontractors must be specified in the applicable Order and Vendor will be solely responsible for all fees and expenses payable to each subcontractor. Vendor's use of any subcontractor shall not relieve Vendor of its representations, warranties or obligations under this Agreement and Vendor shall require that all subcontractors comply with the terms of this Agreement, including confidentiality requirements. Vendor remains directly responsible for the performance of its subcontractors and the acts or omissions of Vendor's subcontractors shall be deemed to be the acts or omissions of Vendor to the same extent as if such acts or omissions were by Vendor or its employees.

4.15 Quality Assurance. Vendor shall conduct quarterly independent internal quality assurance activities to help ensure that the Services are performed with a high degree of professional quality and reliability and shall provide reports and results of the same to Trinity upon request. The work performed by Vendor in respect of such quality assurance activities is included in the Services Exhibit as a fee based service.

4.16 Cooperation. All Services provided by Vendor under this Agreement shall be performed in a manner designed to minimally interfere with Trinity's ongoing business operations. Vendor acknowledges that Trinity receives technology services from other vendors. Vendor agrees to reasonably cooperate and work in good faith with Trinity and its other third party vendors as directed by Trinity.

4.17 Forced Labor. Vendor represents and warrants that neither it, nor any of its subcontractors, will utilize slave, prisoner or any other form of forced or involuntary labor in the performance of Services under this Agreement.

4.18 Nondiscrimination. Vendor agrees that in the performance of its Services under this Agreement, it will not discriminate against any person or entity because of race, color, religion, sex, national origin or any other characteristic protected from discrimination as set forth in the Applicable Laws.

4.19 Vendor Diversity. Vendor acknowledges that Trinity and its Affiliates are committed to vendor diversity. Upon request, Vendor agrees to provide information about Vendor's efforts to create/maintain a diverse workforce and any efforts to contract with subcontractors, suppliers and agents that meet the requirements for certification as Minority and Women Owned Business Enterprises.

5. Representations and Warranties

5.1 Services. Vendor represents and warrants to Trinity that it has the skills, expertise and resources to perform, and that it will perform, the Services: (i) in a timely, professional and workmanlike manner; and (ii) in accordance with industry standards with respect to level of skill, care and diligence; provided, however, that where the Agreement (including any Order) specifies a particular standard or criteria for performance (*e.g.*, an SLA), this warranty is not intended to and does not diminish that standard or criteria for performance. Vendor agrees that any Services warranty re-work will be performed by Vendor Personnel at no additional cost or expense to Trinity.

5.2 Software and Subscriptions. Vendor warrants that Software and Subscriptions will perform substantially in conformance with the functional specifications in the then-current Documentation, provided that, in the case of Software, Trinity maintains active enrollment in Maintenance. This warranty does not apply to any non-conformance to the extent caused by use of the Software or Subscription that is not in accordance with this Agreement or the Documentation provided by Vendor. If the Software or Subscription fails to operate as warranted in this Section and Trinity notifies Vendor in writing of the nature of the non-conformance, Vendor will use commercially reasonable efforts to promptly repair or replace the non-conforming Software or Subscription without charge. The foregoing provides Trinity's sole and exclusive remedy for breach of this warranty.

5.3 Disabling Codes. Vendor represents and warrants to Trinity that: (a) the ASP Services do not contain, and (b) Vendor shall not introduce into the ASP Services or any system of Trinity or its Affiliates via any Vendor-provided medium, any virus, worm, trap door, back door, timer, clock, counter or other

limiting routine, instruction or design that would damage or erase data or programming, disrupt use of the ASP Services or otherwise cause any software, service or system to become inoperable or incapable of being used in the full manner for which it was designed and created (each, a "Disabling Code"). If Vendor Personnel are the source of any such Disabling Code, at its sole cost and expense, Vendor shall, as applicable: (a) take all steps necessary to test for the presence of Disabling Codes, (b) furnish to Trinity ASP Services without the presence of the Disabling Code, and (c) restore and/or reconstruct (or bear the cost of restoring and/or reconstructing) any and all data and programming lost by Trinity as a result of such Disabling Code (such restoration shall include, if needed, on-site technical assistance to extract data from corrupted data files, restoration from backup media, data log analysis, and the like). The foregoing provides Trinity's sole and exclusive remedy for breach of this warranty.

5.4 Intellectual Property. Vendor represents and warrants to Trinity that the ASP Services and Trinity's receipt or use of the ASP Services in accordance with the terms of the Agreement does not and shall not infringe upon, or constitute a theft or misappropriation of, any patent, copyright, trademark, trade secret or other Intellectual Property Rights, or any other proprietary right, of any third party.

5.5 Performance of Services in the United States. Vendor represents and warrants to Trinity that Vendor shall not (a) perform any of its obligations under the Agreement from locations, or using employees, contractors and/or agents, situated outside the United States, or (b) directly or indirectly (including through the use of subcontractors) transmit any Trinity Data outside the United States, or (c) allow any Trinity Data to be accessed by Vendor Personnel from locations outside the United States or transmitted to locations outside the United States. Vendor represents and warrants to Trinity that the primary, backup, disaster recovery and other data center sites for the Host Computer System will be provided, at all times, from locations in the United States.

5.6 Disclaimer. EXCEPT FOR THE REPRESENATIONS AND WARRANTIES SET FORTH IN THIS SECTION 5, VENDOR EXPRESSLY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, WHETHER EXPRESS, IMPLIED, OR STATUTORY (BY ANY TERRITORY OR JURISDICTION) TO THE EXTENT PERMITTED BY LAW, AND FURTHER VENDOR EXPRESSLY EXCLUDES ANY WARRANTY OF TITLE, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. Vendor shall have no obligations under these warranties to the extent a breach of such warranty results from modifications to Blackbaud Solutions, except for the modifications made by Vendor or its agents, modifications authorized in writing by Vendor, or applications made by or on behalf of Trinity or Trinity Affiliates using the Blackbaud Tools within the scope of Section 4.1.1.

6. TERM AND TERMINATION

6.1 Term. The term of this Agreement will be commence on the Effective Date and continue for three (3) years (the "Initial Term") unless terminated in accordance with this Section 6. This Agreement will automatically renew for additional one (1) year terms (each, a "Renewal Term") at the end of the Initial Term or applicable Renewal Term unless Trinity notifies Vendor in writing of its intention not to renew this Agreement at least ninety days (90) days prior to the start of the applicable Renewal Term. The term of each Order (for each Order, the "Order Term") shall be specified therein. Subscriptions and Maintenance for Licenses shall renew in accordance with Section 4.2.2

6.2 Termination for Cause.

6.2.1 Trinity or Vendor may terminate this Agreement in its entirety or with respect to individual Orders upon written notice to the other in the event that the other Party materially defaults in performing its obligations under this Agreement and the default has not been substantially cured within thirty (30) days following receipt by the defaulting party of written notice of default (each, an "Event of Default").

6.2.2 In addition, the following events shall be considered an Event of Default for which Trinity shall have the right to terminate all or any portion of the applicable Order without further payment or liability upon written notice to Vendor: (i) A Chronic Service Issue; or (iii) any other breach or occurrence for which a termination right is expressly set forth in the Agreement. Trinity's failure to terminate an Order, in whole or in part, immediately for any of the foregoing reasons shall not constitute waiver of Trinity's right to terminate the Order for such reasons.

6.2.3 Trinity or Vendor may immediately terminate this Agreement, including any Orders, upon written notice to the other in the event a petition in bankruptcy is filed by or against the other or the other shall make an assignment for the benefit of creditors or take advantage of any insolvency or other laws affording protection against creditors.

6.3 Effect of Termination.

6.3.1 Termination of this Agreement shall not effectuate a termination of each Order then in effect and not otherwise expressly terminated. The terms and conditions set forth herein shall continue in effect with respect to such Order until their expiration or termination as set forth herein.

6.3.2 Upon termination of this Agreement or termination of an Order for a Blackbaud Solution, Vendor may immediately cease providing the terminated offering. Vendor will return all Trinity Data (including, without limitation, Trinity's database where Vendor hosts Trinity's database), in a mutually agreed format upon termination at no cost. If this Agreement is terminated for any reason, Trinity shall nonetheless be obligated to pay Vendor upon such termination any and all undisputed, accrued and unpaid fees and expenses due and payable to Vendor as of the date of termination.

6.3.3 Upon termination of this Agreement and/or any Order by Trinity for any reason pursuant to Section 6, Vendor shall reasonably cooperate with Trinity in the orderly and efficient completion and/or transfer of applicable Services including any knowledge transfer requested by Trinity and return of all Trinity Data in a mutually agreed format, at no cost to Trinity.

6.4 Survival. The termination of this Agreement or any Order, whether for breach or otherwise, shall be without prejudice to any claims for damages or other rights against the other Party that preceded termination. Any provision of this Agreement which can reasonably be construed to survive the expiration or termination of this Agreement shall survive such expiration or termination and shall not relieve either party of its obligations to observe, keep and perform those surviving provisions. Without limitation, the following provisions shall survive the expiration or termination of this Agreement: Service Requirements, Remedies, Compliance with Laws, Audit, Confidentiality and Security, Insurance and Indemnification. Any limitation in an Order that restricts in any way the applicable statute of limitations or the period of time in which any Affiliate may bring a claim is null, void and of no effect.

7. CONFIDENTIALITY AND SECURITY

7.1 Duty of Confidentiality. The Receiving Party shall hold the Confidential Information of the Furnishing Party in strictest confidence using the same or greater degree of care it uses with its own most sensitive information (but in no event less than a reasonable degree of care) and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give or disclose such information to third parties or use such information for any purposes whatsoever other than the performance of this Agreement or as expressly set forth in this Agreement. The Receiving Party shall limit access to Confidential Information of the Furnishing Party to only those of its employees, agents and contractors having a need to know in connection with this Agreement or the provision or receipt of the Services, as applicable. The Receiving Party shall advise all of its employees, agents and contractors who may be exposed to the Confidential Information of the Furnishing Party of their obligations to keep such information confidential in accordance with this Agreement. The Receiving Party shall be responsible for any breach of confidentiality provisions by such employees, agents and contractors. The Receiving Party shall, upon expiration or termination of this Agreement to which any Confidential Information relates or otherwise upon demand, at the Furnishing Party's option, either return to the Furnishing Party or destroy (in each case to the extent permitted by Applicable Law and to the extent commercially practicable) and certify in writing to the Furnishing Party the destruction of any and all Confidential Information of the Furnishing Party, whether in hard copy or electronic format and whether standalone or included in any other materials or documents, in such Receiving Party's possession, provided, however, that the Receiving Party may retain such limited Confidential Information to the extent required for record retention and audit purposes and subject to the terms of this Agreement.

7.2 Exclusions to Duties of Confidentiality. The foregoing duties of confidentiality shall not apply to any Confidential Information that a Receiving Party can show: (i) was, at the time of disclosure, or has later become available to the public through no breach of this Agreement; (ii) was obtained from a third party lawfully in possession of such information that had the legal right to disclose the information without it being subject to a continuing obligation of confidentiality; (iii) was developed by the Receiving Party independently of and without reference to any Furnishing Party's Confidential Information; or (iv) was, at the time of disclosure, already in such Receiving Party's possession prior to direct or indirect disclosure pursuant to this Agreement (or any predecessor agreement between the Parties governing the confidentiality of such information) without restriction and was not generated in the course of, or in connection with, the Services.

7.3 Disclosure Required by Law. If a Receiving Party is requested or required to disclose all or any part of any Confidential Information of the Furnishing Party by legal or administrative process or by law, rule or regulation, the Receiving Party shall, to the extent practicable and subject to Applicable Laws, give prompt written notice of such request to the Furnishing Party and shall give the Furnishing Party the opportunity to seek an appropriate confidentiality agreement, protective order or modification of any disclosure or otherwise intervene, prevent, delay or otherwise affect the response to such request and the Receiving Party shall reasonably cooperate in such efforts. In the event that such relief is not timely obtained, the Receiving Party shall disclose only that portion of the information sought which its counsel advises that it is legally required to disclose after consultation with the Furnishing Party.

7.4 Pricing Information. Trinity shall have the right to use Vendor pricing information for internal analyses and for creating pricing evaluations for disclosure to its Affiliates. Trinity shall also have the right to disclose such information to third parties for performance of such analysis pursuant to a confidentiality

agreement. Trinity shall have the right to disclose the terms of this Agreement to its Affiliates and to also provide copies and/or summaries of this Agreement to potential purchasers of Trinity or an Affiliate pursuant to a confidentiality agreement. Trinity shall have the right to provide pricing information to third party e-commerce companies which process orders between Trinity and Vendor pursuant to a confidentiality agreement.

7.5 Security. Vendor shall at all times have in effect a comprehensive information security program that includes reasonable and appropriate technical, administrative and physical security measures aimed at protecting such information from unauthorized access, disclosure, use, alteration or destruction, and that reflects industry-leading practices, including: (i) implementing a documented and auditable change management program; (ii) segregating production and development environments, with non-public data relating to clients limited to the production environment; (iii) regular information security training and awareness programs throughout Vendor; (iv) appropriate governance and oversight of information security program activities; (v) regular independent reviews and audits; (vi) a robust vendor risk-management program; (vii) well-documented control processes with corresponding written procedures; and (viii) comprehensive and regular monitoring of vulnerabilities and security risks. Promptly following Trinity's request from time to time, Vendor shall provide Trinity with information regarding Vendor's information security program. Vendor shall promptly notify Trinity of any security breach involving Trinity Data, including without limitation any actual or suspected theft, accidental disclosure, or loss of any Trinity Data and/or any unauthorized intrusions into the facilities or secure systems which contain Confidential Information. In addition, Vendor shall comply with the requirements of all applicable security breach notification statutes.

7.6 Business Associate Obligations. To the extent applicable to this Agreement, Vendor shall execute and comply the form of Business Associate Agreement attached hereto as the HIPAA Exhibit. Notwithstanding any contrary terms that may be contained in the Agreement, the terms set forth in the Business Associate Agreement shall govern the handling (including permitted uses and disclosures) of that portion of Trinity Data that is PHI.

7.7 Mutual Publicity. Neither Party may use the name, logo or other identifier of the other Party in any advertising, promotion, publicity, user lists or customer lists, or websites or for any other public purpose, unless a Party has received prior written approval from an authorized representative of the other Party.

7.8 Equitable Relief. Vendor acknowledges that Trinity shall be entitled to seek equitable relief, including, without limitation, injunctive relief and specific performance, without the requirement to post a bond, in the event of any breach or threatened breach of the provisions of this Section 7 by Vendor.

8. COMPLIANCE WITH LAWS

8.1 General Compliance. Vendor shall perform the Services and its obligations under this Agreement in a manner that complies with all applicable federal, state and local laws, rules, regulations and standards, including, without limitation, the standards of the Centers for Medicare and Medicaid Services, The Joint Commission, and those relating to environmental matters, wages, hours and conditions of employment, discrimination, occupational health/safety and motor vehicle safety ("Applicable Law"). Vendor shall take all measures to promptly remedy any violation(s) of Applicable Law in the performance of the Services and its obligations under this Agreement, and shall promptly notify Trinity

of any violation(s) thereof. Vendor shall obtain at its own cost any and all necessary consents, licenses, approvals, and permits required for the provision of Services by Vendor and its Personnel.

8.2 Warranty of Non-exclusion. Vendor represents and warrants to Trinity that neither Vendor nor any of the Vendor Personnel is listed on the United States Excluded Parties List, the HHS Office of Inspector General List of Excluded Individuals/Entities, the United States Department of the Treasury's Office of Foreign Assets Control's list of Specially Designated Nationals and Blocked Persons, or any replacement lists. Vendor further represents and warrants that it searches all such lists when and as recommended by the applicable agencies. Vendor shall notify Trinity immediately to the extent the foregoing representations and warranties are or become untrue.

8.3 Discounts. If applicable to its performance of this Agreement, Vendor shall comply at all times with the regulations issued by the U.S. Department of Health and Human Services published at 42 CFR 1001, and which relate to Vendor's obligation to report and disclose discounts, rebates and other price reductions for Services purchased under this Agreement. Where a discount or other reduction in price of the Services is applicable, the Parties also intend to comply with the "safe harbor" regulations regarding discounts or other reductions in price set forth at 42 C.F.R. §1001.952(h) and Vendor shall cooperate in good faith in ensuring such compliance.

8.4 Corporate Compliance. Trinity maintains and enforces a Corporate Compliance Program, which includes detailed provisions for detecting and preventing fraud, waste, and abuse. Trinity may provide Vendor with such information on its compliance program (including then applicable policies and procedures) that it believes apply to its business relationship with Vendor, which at a minimum includes the Standards of Conduct and Vendor Code of Conduct, available at http://www.trinity-health.org/documents/VendorCodeofConduct.pdf. When and where applicable, Vendor agrees to comply with said policies and procedures.

8.5 Medicare Records Access Requirements. If this Agreement is subject to the Medicare statutes and regulations governing access to books and records of subcontractors, then for a minimum of six (6) years after the expiration of this Agreement, Vendor shall retain and allow the authorized representatives of the Comptroller General and the Department of Health and Human Services access to this Agreement and to the books, records, and other documents of Vendor that are necessary to verify the nature and costs paid to Vendor pursuant to this Agreement. If Vendor carries out any duties of this Agreement by means of a subcontractor, including any organization related by ownership or control with Vendor, and the cost or value of which is $10,000 or more over a twelve (12) month period, then Vendor shall require the subcontractor to comply with the provisions of this Section. In the event Vendor receives a request for access, Vendor agrees to promptly notify Trinity.

8.6 Meaningful Use Without limiting Vendor's Support Services obligations, Vendor shall ensure that the ASP Services are compliant, and provided in conformance, with the criteria for meaningful use for an electronic health record, including the privacy and security criteria. Vendor also shall ensure that the ASP Services are compliant with regulations applicable to payment card industry compliance, data breach reporting, patient rights and federal and state electronic records regulations. Vendor shall comply with Trinity's interpretation of state and federal regulations of which Vendor has been informed in writing by Trinity, unless Vendor advises Trinity of its disagreement with Trinity's interpretation, in which case the Parties shall cooperate in good faith to resolve any such dispute in accordance with Section 12.7.

9. INTELLECTUAL PROPERTY; OWNERSHIP

9.1 Trinity Owned Materials. Trinity reserves all ownership and other rights of any nature in and to the works of authorship, materials, information and other intellectual property created by Trinity personnel or contractors prior to the Effective Date or independently of the Agreement (whether created prior to, on, or after the Effective Date), plus all modifications, changes, supplements, enhancements, or improvements to, or derivations of, any of the foregoing.

9.2 Vendor Owned Materials. Vendor reserves all ownership and other rights of any nature in and to the works of authorship, materials, information and other intellectual property created by Vendor prior to the Effective Date or independently of the Agreement (whether created prior to, on, or after the Effective Date), plus all modifications, changes, supplements, enhancements, or improvements to, or derivations of, any of the foregoing ("Vendor-Owned Materials").

9.3 Ownership of Deliverables. Subject to the rights of Trinity set forth above in Section 9.1 and the restrictions in Section 9.4, Vendor has all right, title, and interest in and to any expressions and results of Blackbaud Solutions, the work, findings, analyses, conclusions, opinions, recommendations, ideas, techniques, know-how, designs, programs, tools, applications, interfaces, enhancements, other technical information, and all derivatives of the foregoing created in connection with this Agreement ("Work Product"). Vendor grants to Trinity a nonexclusive, fully paid-up license to use Work Product, solely to the extent necessary for Trinity and its end users to use Blackbaud Solutions in accordance with this Agreement. If Trinity provides any feedback, comments, suggestions, ideas, requests, or recommendations for modifications or improvements to Vendor relating to the Blackbaud Solutions ("Feedback"), Trinity hereby assigns all right, title, and interest in any such Feedback to Vendor to be used for any purpose. All rights not expressly granted to Trinity hereunder are reserved by Vendor.

9.4 Limited Data Use. Vendor may not use any Trinity Data, documents, know-how, methodologies, software or other materials provided to Vendor for any purpose except to the extent necessary to provide the Services during the Term of this Agreement. Vendor shall not sell, assign, lease, disseminate, or otherwise dispose of Trinity Data or any part thereof to any other person, and Vendor shall not commercially exploit any part of the Trinity Data, even if de-identified.

10. INSURANCE AND INDEMNIFICATION

10.1 Insurance. During the Term of this Agreement, Vendor shall carry and maintain at its own cost, with companies that are rated a minimum of "A-" in Best's Insurance Guide or are otherwise reasonably acceptable to Trinity, the following insurance coverage types with the following minimum primary limits (or umbrella liability or excess liability coverage meeting such minimum coverage):

10.1.1 Professional Services Errors & Omissions Liability insurance with a limit of not less than One Million Dollars ($1,000,000) per claim and Three Million Dollars ($3,000,000) in the annual aggregate;

10.1.2 Commercial General Liability insurance, insuring against bodily injury, property damage, contractors' completed operations and contractual liability with a combined single limit of not less than five million dollars ($5,000,000) per claim and Ten Million Dollars ($10,000,000) in the annual aggregate. Trinity shall be named as an additional insured on this policy;

10.1.3 Worker's Compensation and Employer's Liability insurance, with statutory limits for workers' compensation and Employer's Liability limits of one million dollars ($1,000,000) per claim and in the annual aggregate;

10.1.4 Automotive liability covering all vehicles owned, non-owned, hired and leased while used on Trinity business with minimum automotive liability insurance limits of one million dollars ($1,000,000) per claim and in the annual aggregate;

10.1.5 Network liability (privacy) insurance in an amount of five million dollars ($5,000,000) single limit to cover civil, regulatory and statutory damages as a result of actual or alleged breach, violation or infringement of right to privacy, consumer data protection law, confidentiality or other legal protection for personal information. Trinity shall be named as an additional insured on this policy.

The insurance coverages set forth in this Section 10.1 shall not be reduced below the minimum coverages set forth above or cancelled without thirty (30) days prior written notice to Trinity.

10.2 Proof of Insurance. Vendor shall provide Trinity with a copy of the certificates of insurance required under this section no later than the Effective Date of this Agreement. Vendor shall provide Trinity with updated certificates of insurance upon request to evidence Vendor's continued compliance with the terms of this Agreement.

10.2.1 In the event that any of the above-described insurance policies are written on a claims-made basis, then such policy or policies shall be maintained during the Term of this Agreement and for a period of not less than three (3) years following the termination or expiration of this Agreement.

10.2.2 The provisions of this Section shall not be deemed to limit the liability of Vendor hereunder or limit any right that Trinity may have including rights of indemnity or contribution. The insurance obligations under this Section are mandatory; failure of Trinity to request certificates of insurance or insurance policies shall not constitute a waiver of Vendor's obligations and requirements to maintain the minimal coverage specified. Vendor shall ensure and be solely responsible for ensuring that its subcontractors maintain insurance coverage at levels no less than those required by applicable law and customary in the relevant industry.

10.3 General Mutual Indemnification. Each Party (the "Indemnifying Party") shall defend and indemnify the other Party, its successors, assigns, directors, officers, and employees (collectively, the "Indemnitees") from and against any third party claim arising from the Indemnifying Party's gross negligence or willful misconduct in connection with such Indemnifying Party's performance of this Agreement. If the third party claim is caused by the gross negligence or willful misconduct of both Vendor and any of the Trinity Indemnitees, the apportionment of said claim shall be shared between Vendor and Trinity Indemnitees based upon the comparative degree of each other's gross negligence or willful misconduct, notwithstanding the existence of any applicable state laws governing comparative negligence or fault, and each shall be responsible for its own defense and costs including but not limited to the cost of defense, attorneys' fees and witnesses' fees and expenses incident thereto.

10.4 Intellectual Property Indemnification.

10.4.1 Vendor shall defend and indemnify the Indemnitees of Trinity against any third party claims that Blackbaud Solutions as delivered or made available to Trinity infringe or misappropriate any United States or Canadian Intellectual Property Right. In the event that Trinity's use of or access to any Blackbaud Solution becomes subject to a third party claim of infringement or misappropriation, Vendor shall, in its reasonable judgment and at its option and expense: (a) obtain for Trinity the right to continue using the affected Blackbaud Solutions; (b) replace or modify the Blackbaud Solution so that is becomes non-infringing while giving equivalent performance; or (c) if Vendor cannot obtain the remedies in (a) or (b), as its sole obligation, Vendor or Trinity may terminate the License or Subscription to the infringing Blackbaud Solution and Vendor shall refund the License fee (adjusted for depreciation on a thirty-six (36) month basis) and any pre-paid Subscription or Maintenance fees related to such Blackbaud Solution.

10.4.2 Vendor's indemnification obligations under this Section 10.4 shall not extend to any claim to the extent such claim results from (i) modifications made by or on behalf of a Trinity Indemnitee without the prior written consent of Vendor, unless (a) such infringement, misappropriation or other violation would still exist in the absence of such modification, or (b) such modification was made at the request, recommendation, or with the knowledge of Vendor; (ii) the combination with any products or services from third party vendors, unless (a) such infringement, misappropriation or other violation would still exist in the absence of such combination, or (b) such combination was agreed to by Vendor or was made at the request, recommendation, direction, or with the knowledge of Vendor; (iii) infringing information, data, software, applications, services, or programs created or furnished by Trinity or by persons other than Vendor or its agents; or (iv) use by Trinity of the Blackbaud Solution other than in accordance with this Agreement, any Documentation or any delivered documentation under a Statement of Work.

10.4.3 This Section 10.4 states the entire liability of Vendor with respect to any indemnification for third party claims of Intellectual Property Right infringement.

10.5 Trinity Indemnification. Trinity shall defend and indemnify the Indemnitees of Vendor from and against any third party claim made against Vendor Indemnitees arising from Trinity's breach of the AUP or Sections 4.6 (Trinity Control) or 4.7 (Prohibited Uses).

10.6 Indemnification Procedures. The applicable Indemnitee shall give the Indemnifying Party prompt written notice of any claims for indemnification and the such Indemnitee agrees to permit the Indemnifying Party to control the defense of any such claim, including the right to settle; provided however, that the Indemnifying Party will not settle any such suit or claim without such Indemnitee's prior written consent, which shall not be unreasonably withheld.

11. LIMITATION OF LIABILITY

11.1 Damages. EXCEPT FOR DAMAGES FINALLY JUDICIALLY AWARDED TO A THIRD PARTY IN CONNECTION WITH A CLAIM FOR WHICH A PARTY HAS AN INDEMNIFICATION OBLIGATION UNDER THIS AGREEMENT, IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTIAL, INDIRECT, EXEMPLARY, SPECIAL OR PUNITIVE DAMAGES (INCLUDING, WITHOUT LIMITATION, LOSS OF REVENUES, PROFITS OR OPPORTUNITIES) WHETHER ARISING OUT OF BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE REGARDLESS OF

WHETHER SUCH DAMAGE WAS FORESEEABLE AND WHETHER OR NOT SUCH PARTY HAS BEEN ADIVSED OF THE POSSIBILITY OF SUCH DAMAGES.

11.2 Limitation of Liability. EXCEPT AS OTHERWISE PROVIDED IN SECTION 11.3, IN NO EVENT WILL EITHER PARTY'S LIABILITY ARISING OUT OF THIS AGREEMENT, WHETHER ARISING OUT OF BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE EXCEED TWO TIMES (2X) THE AMOUNT OF FEES PAID OR PAYABLE BY TRINITY FOR THE BLACKBAUD SOLUTION FROM WHICH THE CLAIM AROSE DURING THE TWELVE (12) MONTHS PRECEDING THE CLAIM.

11.3 Limitations Not Applicable. The limitations set forth in Section 11.2 shall not apply to: (i) a Party's indemnification obligations under Sections 10.3, 10.4 and 10.5; (ii) third party claims arising out of (a) a Party's failure to comply with its obligations in respect of confidentiality and security under Section 7 (Confidentiality and Security) or (b) Vendor's breach of any Business Associate Agreement between the Parties; (iii) third party claims arising out of a Party's failure to comply with Applicable Laws; (iv) death or bodily injury or damage to real or tangible personal property resulting from a Party's negligence or willful misconduct; and (v) damages or other liabilities arising out of theft, embezzlement, gross negligence, willful misconduct, intentional breach or fraud of a Party or any of the Vendor Personnel.

12. MISCELLANEOUS

12.1 Mission. Vendor acknowledges that Trinity is a non-profit, Catholic health system, which is devoted to a ministry of healing and providing quality medical care to the poor and underserved.

12.2 Independent Contractor Relationship. In performing any and all of its obligations under this Agreement, Vendor shall at all times and for all purposes be and remain an independent contractor and in no case and under no circumstances shall Vendor or any of its Personnel, be considered or otherwise deemed to be employees or agents of Trinity or its Affiliates for any purposes whatsoever. This Agreement is not intended to establish a partnership, joint venture, employer-employee or joint employer relationship. Vendor is responsible for all salaries, payroll taxes and other taxes, benefits, fees, and other charges or insurance required by any federal, state and local law, statute or regulation (including, but not limited to, unemployment taxes, Social Security contributions, workers' compensation premiums and all similar taxes, payments, and any penalties and fines relating thereto), attributable to each of its Personnel. Neither Vendor nor any of its Personnel shall have any power or authority to bind Trinity or its Affiliates to contractual or other obligations.

12.3 Business Review Meetings. Each Party shall designate an individual who will have overall responsibility for managing the relationship created through the Agreement (for each Party, the "Relationship Manager"). The Relationship Managers and other appropriate representatives from each party shall meet at least once every six (6) months to participate in regularly scheduled performance review meetings for the purpose of reviewing the performance of Vendor's Services and its Personnel and compliance with the Agreement SLAs, terms and pricing. The Parties will also discuss the availability and implementation of any new Services that Trinity may wish to consider having Vendor implement. Unless otherwise agreed to by the Parties, business review meetings will be held by telephone. All time and expenses associated with Vendor's participation in business review meetings will be the responsibility of Vendor, including, without limitation, travel, lodging and meals.

12.4 Audit. Vendor shall maintain complete and accurate books, records, and data as necessary to support the charges and expenses invoiced hereunder and to permit Trinity or its designee to verify the accuracy of such amounts. Vendor shall permit Trinity or its designated agents, upon reasonable notice and at reasonable times, to inspect Vendor's records, invoices, processes and procedures as they relate to the Services furnished pursuant to this Agreement and any use of Trinity Data. Such audits shall be limited to once per calendar year and shall be conducted upon reasonable advance notice during regular business hours and in such a manner as not to unduly interfere with Vendor's operations.

12.4.1 Operational and Security Audits. Trinity shall have the right to request information from Vendor in respect of Vendor's performance of the Services and its other obligations hereunder, including information related to: (i) the integrity of Trinity Data; (ii) the systems that process, store, support and transmit Trinity Data; (iii) the internal controls implemented by Vendor as they relate to the Services; (iv) the security, disaster recovery and back-up practices and procedures as they relate to the Services; (v) Vendor's performance against the SLAs; (vi) Vendor's measurement, monitoring and management tools, and (vii) applicable legal, regulatory and contractual requirements. In addition, upon request by Trinity, Vendor will timely provide to Trinity copies of any independently conducted third-party audit or assessment report that includes testing of Vendor's general and technology-based controls, such as SSAE16/SAE3402, SysTrust, and Payment Card Industry (PCI) Data Security Standard (DSS) provided that such audit or assessment report is of a type Vendor generally makes available to its customers.

12.4.2 Vendor Audits. If Vendor believes that Trinity has exceeded any Scope-of-Use Limitations, Vendor shall promptly notify the Trinity Relationship Manager in writing and provide Trinity with a copy of the user report substantiating the specific degree of non-compliance for Trinity's review and verification. The Relationship Managers shall endeavor to confirm any excess use within thirty (30) days of Trinity's receipt of the user report from Vendor and discuss plans to resolve any non-compliance which has been confirmed by the Parties. Within thirty (30) days of any confirmed non-compliance by Trinity, Trinity shall either (i) disable any use in excess of the Scope-of-Use Limitations; or (ii) purchase additional licenses at the fees set forth in the Services Exhibit to the extent necessary to address any non-compliance with the Scope-of-Use Limitations. Based on the foregoing, Vendor waives its right to conduct a review or audit of Trinity's usage of the Services.

12.5 Assignment. The Parties may not assign this Agreement or any Order without the prior written consent of the other Party. Any assignment without the other Party's prior written consent shall be void and have no effect.

12.6 Governing Law. The rights and obligations of the Parties under this Agreement shall be governed in all respects by the laws of the State of Indiana, excluding conflicts of law provisions. The Parties expressly consent to the exclusive jurisdiction of the state and federal courts located in the State of Indiana for any dispute concerning this Agreement and agree not to commence any such proceedings except in such courts. The Parties hereby waive all defenses of lack of personal jurisdiction and forum non conveniens related thereto.

12.7 Dispute Resolution. The Parties shall attempt to settle any claim or controversy arising from the Agreement through negotiation in good faith. If a dispute relating to the Agreement arises between the Parties, the Relationship Managers shall first meet and attempt to resolve the dispute. If the Relationship Managers are unable to resolve the dispute within thirty (30) days after they have

commenced discussions regarding the dispute, the dispute will then be escalated to the appropriate higher-level managers and executives of the Parties, if necessary.

12.8 Essential Services. Vendor acknowledges that Trinity is a provider of essential services, including medical services. Vendor shall develop, test and implement business continuity and disaster recovery plans with respect to its operations.

12.9 Force Majeure. No Party shall be liable to the other party for any failure or delay in performing any term of this Agreement when and to the extent such failure or delay results from acts beyond the affected Party's reasonable control, including, without limitation, acts of God, acts of terrorism, action of governmental authorities, flood, fire or explosion ("Force Majeure Event"). In the event that either Party's performance is delayed or such Party fails to perform its obligations under this Agreement due to a Force Majeure Event, such Party shall (i) promptly notify the other Party in writing of such Force Majeure Event and its expected duration; and (ii) take all reasonable steps to recommence performance of its obligations under this Agreement as soon as possible. Trinity will not be obligated to pay any fees or charges for Services Vendor fails to perform as a result of a Force Majeure Event.

12.10 Notices. All notices required hereunder shall be given in writing and addressed or delivered to the persons specified in this Agreement. Any such notice shall be effective upon depositing the notice in first-class mail or certified mail, return receipt requested, at the addresses below or upon actual receipt. Each Party and Affiliate may change the persons designated to receive notice hereunder by written notice.

Notices to Trinity:
20555 Victor Parkway
Livonia, MI 48152
Attention: Vice President, Supply Chain

Copy to: Trinity Legal Department
20555 Victor Parkway
Livonia, MI 48152
Attention: General Counsel

Notices to Vendor:
2000 Daniel Island Drive
Charleston, SC 29492
Attention: President, Enterprise Customer Business Unit

Copy to: Blackbaud Law Department
2000 Daniel Island Drive
Charleston, SC 29492
Attention: General Counsel

12.11 Waiver. Any waiver of a breach of any provision(s) of this Agreement shall not be deemed effective unless it is in writing and signed by the Party against whom enforcement of the waiver is sought.

12.12 Section Headings. The headings contained in this Agreement are for reference purposes only and will not in any way affect the meaning or interpretation of this Agreement.

12.13 Entire Agreement; Amendment. This Agreement, together with all Orders, Statements of Work, Exhibits, attachments and schedules attached hereto and incorporated herein, constitutes the entire Agreement between the Parties with respect to the subject matter herein and supersedes all prior agreements, arrangements and/or understandings between the Parties with respect to the subject matter herein. The Parties agree that should any conflict or inconsistency arise between the application and/or interpretation of the terms of this Agreement, the following order of precedence shall be followed in resolving any conflicts among the terms of the Agreement: (i) first, and most senior, Applicable Laws; (ii) second, the terms contained in any Order Form; (iii) third, the terms contained in the body of this Agreement including the Exhibits to the Agreement; (iv) fourth, the terms of any Statement of Work; and (v) fifth, the Documentation and applicable support manuals. This Agreement may not be modified or amended other than by an agreement in writing signed by both Parties. Any modification or amendment to the terms of this Agreement made in any Order Form must expressly refer to the provision of this Agreement that is being modified or amended and such modification or amendment shall apply only to that Order Form.

12.14 No Construction Against Drafter. The Parties agree that any principle of construction or rule of law that provides that an agreement shall be construed against the drafter of the agreement in the event of any inconsistency or ambiguity in such agreement shall not apply to the terms and conditions of the Agreement.

12.15 Severability. If any term of this Agreement is invalid, illegal or unenforceable in any jurisdiction, such invalidity or unenforceability shall not affect any other term or provision of this Agreement or invalidate or render unenforceable such term or provision in any other jurisdiction. In such event the Parties shall negotiate in good faith to modify this Agreement so as to effect the original intent of the Parties as closely as possible in a mutually acceptable manner in order that the transactions contemplated be consummated as originally contemplated to the greatest extent possible.

12.16 Remedies Cumulative. Unless expressly stated otherwise in this Agreement, all remedies provided for in this Agreement will be cumulative and in addition to, and not in lieu of, any other remedies available at law, in equity or otherwise.

12.17 Counterparts. This Agreement and any Order may be executed by the exchange of faxed executed copies, certified electronic signatures or copies delivered by electronic mail in PDF or similar format, and any signature transmitted by those means for the purpose of executing this Agreement or any Order shall be deemed an original signature for purposes of this Agreement or any Order. This Agreement or any Order may be executed in two or more counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same instrument.

IN WITNESS WHEREOF, the undersigned authorized representatives of the Parties have executed this Master ASP Services Agreement, effective as of the Effective Date.

TRINITY HEALTH CORPORATION:

By: _____

Name: Marcus B. Shipley

Title: CIO

Dated: 6.18.15

BLACKBAUD, INC.:

By: _____

Name: Brian E. Boruff

Title: President, Enterprise Business Unit

Dated: 06/15/2015

Exhibit A

LIST OF EXHIBITS

Services Exhibit

Order Form Exhibit

Hosting and Service Level Exhibit

ASP Services Exhibit

Testing and Acceptance Exhibit

Support Services Exhibit

HIPAA Exhibit

Travel Policy Exhibit

Services Exhibit

1. Blackbaud CRM Subscription

Blackbaud CRM Subscription Pricing	Price per unit where applicable	Supplier Explanation
Blackbaud CRM - 150 Concurrent Licenses	$420,000 annually	3 year initial contract term. Annual price will remain fixed during the initial 3 year term. Please see MSA for renewal terms.
Pricing model, Enterprise or Per User?	Per User	
Price per user per year for all access user.	$2,800	This per user cost will not increase during the initial 3 year contract term.
Enterprise Price per year for unlimited users.	N/A	
Are users defined as concurrent or named?	Concurrent	
If named user, can named user be reassigned if original user, for any reason, no longer requires system access?	N/A	
Blackbaud CRM Implementation Pricing	**Price per unit where applicable**	**Supplier Explanation**
Blackbaud CRM Implementation	$2,307,400	Please see Blackbaud CRM Implementation SOW. This does not include travel costs.
Blackbaud CRM Training Pricing	**Price where applicable**	**Supplier Explanation**
Provide all required Training costs		Initial training costs are included in the implementation price. Please see Blackbaud CRM SOW.
Provide any optional Training costs	$5000/annually $3500/day	Blackbaud CRM Learn Pass - unlimited web-based training for ongoing end user training Custom Onsite Training for Blackbaud CRM.

<table>
<tr><th>Blackbaud CRM Consulting Pricing</th><th>Price per unit where applicable</th><th>Supplier Explanation</th></tr>
<tr><td>T&M Consulting Rates</td><td>See Rate Card</td><td>
<table>
<tr><th>Service</th><th>Hourly rate</th></tr>
<tr><td>System Architecture</td><td>$ 250</td></tr>
<tr><td>Business Analysis</td><td>$ 250</td></tr>
<tr><td>Business Intelligence & Reporting</td><td>$ 225</td></tr>
<tr><td>Implementation</td><td>$ 225</td></tr>
<tr><td>Data Conversion</td><td>$ 200</td></tr>
<tr><td>Application Development</td><td>$ 250</td></tr>
<tr><td>Training</td><td>$ 200</td></tr>
<tr><td>Engagement Management</td><td>$ 250</td></tr>
<tr><td>Quality Assurance</td><td>$ 225</td></tr>
</table>
The blended hourly rate of $200 will be used for Services provided with respect to the Blackbaud CRM and TeamRaiser implementation project including the rates used for any chargeable Change Orders arising in connection with such project. The $200 hourly rate shall apply during the pendency of the CRM Project and for 6 months following Project Completion. All other services will be scoped using the included rate card.
</td></tr>
</table>

Pricing/Miscellaneous	Price per unit where applicable	Supplier Explanation
Blackbaud Merchant Services (BBMS) - credit card processing	2.598% + .26 per transaction	
Third-party credit card processing	.20 per transaction interconnect fee	Only applicable if Trinity Health opts to use a third party processor rather than BBMS.
Blackbaud Conference for Nonprofits 2015 Registration	$975 - first attendee $925 - additional attendees	Blackbaud is providing 2 complimentary BBCON2015 registrations as part of the Blackbaud CRM Order Form.
Storage Space Overage	$12,000 annually per	

	TB	

2. Blackbaud CRM Perpetual

Blackbaud CRM Perpetual Pricing	Price per unit where applicable	Supplier Explanation
Blackbaud CRM - Site License	$600,000	
Blackbaud CRM - Annual Maintenance	$271,000	Annual maintenance includes TAM, Customer Support and all updates
Pricing model, Enterprise or Per User?	Per User	
Price per user per year for all access user.	N/A	
Enterprise Price per year for unlimited users.	N/A	
Are users defined as concurrent or named?	Concurrent	
If named user, can named user be reassigned if original user, for any reason, no longer requires system access?	N/A	
Blackbaud CRM Implementation Pricing	**Price per unit where applicable**	**Supplier Explanation**
Blackbaud CRM Implementation	$2,307,400	Please see Blackbaud CRM Implementation SOW. This does not include travel costs.

Blackbaud CRM Training Pricing	Price where applicable	Supplier Explanation
Provide all required Training costs		Initial training costs are included in the implementation price. Please see Blackbaud CRM SOW.
Provide any optional Training costs	$5000/annually $3500/day	Blackbaud CRM Learn Pass - unlimited web-based training for ongoing end user training Custom Onsite Training for Blackbaud CRM.
Blackbaud CRM Consulting Pricing	**Price per unit where applicable**	**Supplier Explanation**
T&M Consulting Rates	See Rate Card	

Service	Hourly rate
System Architecture	$ 250
Business Analysis	$ 250
Business Intelligence & Reporting	$ 225
Implementation	$ 225
Data Conversion	$ 200
Application Development	$ 250
Training	$ 200
Engagement Management	$ 250
Quality Assurance	$ 225

The blended hourly rate of $200 will be used for Services provided with respect to the Blackbaud CRM and TeamRaiser implementation project including the rates used for any chargeable Change Orders arising in connection with such project. The $200 hourly rate shall apply during the pendency of the CRM Project and for 6 months following Project Completion. All other services will be scoped using the included rate card.

Pricing/Miscellaneous	Price per unit where applicable	Supplier Explanation
Blackbaud Merchant Services (BBMS) - credit card processing	2.598% + .26 per transaction	
Third-party credit card processing	.20 per transaction interconnect fee	Only applicable if Trinity Health opts to use a third party processor rather than BBMS.
Blackbaud Application Hosting	$275,000 annually	
Storage Space Overage	$12,000 annually per TB	

3. Financial Edge Subscription

Financial Edge Subscription Pricing	Price per unit where applicable	Supplier Explanation
Financial Edge Subscription Pricing	Estimated $148,000 annually	Based on initial conversations: 3 year initial contract term. Annual price will remain fixed during the initial 3 year term. Includes 50 concurrent licenses, managed hosting, and maintenance, support, Technical Account Manager, all updates. Final pricing will be reflected in the Order Form.
Pricing model, Enterprise or Per User?	Per User	
Price per user per year for all access user:	$1,500	This per user cost will not increase during the initial 3 year contract term.
Enterprise Price per year for unlimited users.	N/A	
Are users defined as concurrent or named?	Concurrent	
If named user, can named user be reassigned if original user, for any reason, no longer requires system access?	N/A	

Financial Edge Implementation Pricing	Price per unit where applicable	Supplier Explanation
T&M Consulting Rates	Estimated $385,000 for initial implementation	<table><tr><th>Service</th><th>Hourly rate</th></tr><tr><td>System Architecture</td><td>$ 250</td></tr><tr><td>Business Analysis</td><td>$ 250</td></tr><tr><td>Business Intelligence & Reporting</td><td>$ 225</td></tr><tr><td>Implementation</td><td>$ 225</td></tr><tr><td>Data Conversion</td><td>$ 200</td></tr><tr><td>Application Development</td><td>$ 250</td></tr><tr><td>Training</td><td>$ 200</td></tr><tr><td>Engagement Management</td><td>$ 250</td></tr><tr><td>Quality Assurance</td><td>$ 225</td></tr></table> SOW and final pricing for Financial Edge Implementation Services will be developed through additional conversations between Blackbaud and Trinity using the rate card above unless otherwise noted in the SOW and Order Form.

Financial Edge Training Pricing	Price where applicable	Supplier Explanation
Provide all required Training costs		Initial estimates for custom training costs are included in the implementation price and will be defined in the SOW. Financial Edge Learn is included in the subscription pricing.
Provide any optional Training costs	$3500/day	Custom Onsite Training for The Financial Edge.

Pricing/Miscellaneous	Price per unit where applicable	Supplier Explanation
FE Storage Space Overage	$1200/5 GB	

4. TeamRaiser

TeamRaiser Subscription Pricing	Price per unit where applicable	Supplier Explanation
TeamRaiser Subscription Pricing	$4500 annually	This annual subscription is waived for the 3 year initial contract term.
Pricing model, Enterprise or Per User?	N/A	
Price per user per year for all access user.	N/A	
Enterprise Price per year for unlimited users.	N/A	
Are users defined as concurrent or named?	N/A	
If named user, can named user be reassigned if original user, for any reason, no longer requires system access?	N/A	
TeamRaiser Implementation Pricing	**Price per unit where applicable**	**Supplier Explanation**
TeamRaiser Implementation Pricing	$67,500	Please see SOW for TeamRaiser Implementation detail.
tTeamRaiser Training Pricing	**Price where applicable**	**Supplier Explanation**
Provide all required Training costs		Initial training costs are included in the implementation price and are defined in the SOW.

Provide any optional Training costs	N/A	
TeamRaiser Consulting Pricing	**Price per unit where applicable**	**Supplier Explanation**
T&M Consulting Rates	See Rate Card	

Service	Hourly rate
System Architecture	$ 250
Business Analysis	$ 250
Business Intelligence & Reporting	$ 225
Implementation	$ 225
Data Conversion	$ 200
Application Development	$ 250
Training	$ 200
Engagement Management	$ 250
Quality Assurance	$ 225

Pricing/Miscellaneous	**Price per unit where applicable**	**Supplier Explanation**
Blackbaud Merchant Services (BBMS) - credit card processing	2.598% + .26 per transaction	
Third-party credit card processing	.20 per transaction interconnect fee	Only applicable if Trinity Health opts to use a third party processor rather than BBMS.
TeamRaiser Transaction Fee	5% per transaction	

5. Target Analytics

Target Analytics Estimated Pricing	**Estimated Price per unit where applicable**	**Supplier Explanation**		
		Y1	**Y2**	**Y3**
Custom Models	Principle Giving – 3M records		**$35,000**	**$20,500 (rescreen)**
	ProspectPoint Models including Annual, Major, Planned and Target Gift Range – 3M Records		**$41,000**	
	Batch Screening on top 30,000 records identified through Custom Models		**$15,000**	
WealthPoint for BBCRM	WealthPoint Screening in CRM – unlimited one-off screenings, up to 95k records through batched screenings annually		$77,500	$77,500
Patient Screening	WealthPoint OnTime- 550K patients across 35 RHMs – submitted at RHM level		$111,360	$77,360

Data Enrichment Services	AddressFinder – up to 3M records, run quarterly from CRM		$5,200	$5,200
	AddressAccelerator – up to 3M records, run once annually from CRM		$1,950	$1,950
	Deceased Record Finder – up to 3M records, run once annually from CRM		$6,000	$6,000
	EmailFinder – up to 3M records, run once		$46,750	
Conversion/Lapsed Tags	Conversion TAGS - 500k records/quarterly			$11,500
	Lapsed TAGS – 500k records/quarterly			$11,500
Target Analytics Options		**Supplier Explanation**		
Target Analytics Annual Pricing	Pricing above is estimated based on initial conversations with Trinity Health. Blackbaud and Trinity Health will refine Target Analytics Services through further conversations based on Trinity Health's needs and will be reflected in the Order Form and Scope of Work for Target Analytics.			

Order Form Exhibit

See attached form of Blackbaud Order Form.

Exhibit A

Hosting and Service Level Exhibit

See attached Blackbaud Hosting Service, Service Description for Enterprise Clients.

Exhibit A

ASP Services Exhibit

1. General. Vendor reserves the right to change the configuration of its Host Computer System, provided that such changes do not adversely affect the security or functionality of the System or the use of or access to the System by Trinity and/or the Authorized Users. To the extent reasonably possible, Vendor shall notify Trinity in advance of any plans to change such configuration.

2. Disaster Recovery/Business Continuity. The following outlines the failover solution assuming a disaster or failure of Vendor's primary data center. A disaster is defined as an event, or the threat of an event, that could render Vendor's primary facility completely inoperative for an extended period of time. In the event of a true site failover to our secondary data center, once the primary data center is restored to full functionality, the goal will be to return Trinity's production database back to the primary data center within approximately seven (7) days. Upon return to the primary data center, Vendor will then re-establish Trinity's disaster recovery failover capabilities.
    a. Disaster Criteria
        i. A disaster is defined as an event, or the threat of an event that could render Vendor's primary data center or the client's system completely inoperative.
        ii. Duration of more than 24 hours.
    b. Disaster Response
        i. If this situation was to present itself, Vendor and Trinity will discuss the situation and together Vendor will declare a disaster. Vendor will secure replacement hardware and restore Trinity's systems using the off-site backups at a new hosting facility.
        ii. Recovery Time Objective (RTO) – As soon as possible with a goal of returning Trinity to full operations within thirty (30) days.
        iii. Recovery Point Objective (RPO) – Most recent available backup. Vendor will use the most recent backup available with any subsequent transaction logs available to restore the database. Vendor will do best effort to bring the database to as close to the point of disaster as possible.
        iv. Once a disaster is declared Vendor is no longer subject to downtime penalties.
    c. Standard Disaster Recovery Fees: Included with Hosting Fees.

3. Security Requirements.
    a. Industry and Security Standards. Vendor shall maintain the security and integrity of the Host Computer System and ASP Services consistent with industry standards for comparable services, including maintaining access controls, firewalls, wireless and mobile device and storage security, virus scanning/protection software, anti-malware software, encryption of data in transport and storage (including backup data), and network security intrusion protection systems. Vendor shall not take any action that could jeopardize the confidentiality, integrity, availability or security of the System or Trinity Data.

    b. Security Program and Controls. Vendor shall maintain a security program with an identified security official responsible for the operations and performance of the program and shall notify Trinity of any security certifications it receives and any changes to the program. Annually, Vendor shall provide Trinity documentation of the controls and currency of the controls for website security, physical security of the data center and equipment, timely responses to and notification of security incidents/issues,

database and transmission encryption, data quality/corruption prevention, timely return/destruction of data and restrictions and security of use of portable media.

c. Security Policies. Vendor shall maintain information security policies that specifically address the confidentiality, integrity and availability of its facilities, systems and the information in its possession and control. Vendor's security policies must be made available to Trinity upon request.

d. Identity Authentication and Access.
   i. End-User Password Security. Vendor shall ensure that the ASP Services incorporate end user password security by individual user for access and preclude unauthorized users from accessing Trinity Data.
   ii. Secure Access. Vendor shall provide access to the ASP Services via a secured methodology, consistent with industry standards set by NIST.
   iii. Unique Identification. Unique user accounts will be assigned to each user. The account will identify each user. The sharing of user accounts is prohibited. The user account will be commonly known as the user ID. This user ID will be required for access to the ASP Services.
   iv. Authentication. Each user account will be combined with a personal password that authenticates the individual user. Passwords will be constructed with password attributes designed to balance organizational risk, usability, system security and technical feasibility.
   v. Minimum Length and Composition. The password will be a minimum of eight (8) characters in length with at least one (1) alphabetic and one (1) numeric character.
   vi. Initial Password Requirement. Users are required to change their initial password at the time of the initial logon.
   vii. Password Reset. User identity verification must occur prior to password resets. If a password is reset by personnel other than the user, the password must be immediately changed by the user upon first use.
   viii. Expiration. The password will expire within one hundred eighty (180) days.
   ix. History. A minimum of six (6) passwords must be kept in history so that they cannot be re-used during a password change event.
   x. Changes. The user will be provided a mechanism to change his/her password.
   xi. Suspension and Reset. A user will be locked out of the System after six (6) or fewer consecutive invalid authentication attempts.
   xii. Timeout. The ASP Services will timeout and require authentication after fifteen (15) minutes of inactivity. The System will show the last time and date the user logged in.

e. Data Access Controls. Vendor Personnel shall be identified by a unique user ID and password as a condition to gaining access to the Vendor Systems.

4. Auditing and Monitoring - Access Logs. Vendor shall ensure that its security program includes review and examination of system access and event logs, and/or activities to evaluate the utilization levels, efficiency and technical capabilities of the host computer network and each user's compliance with the Agreement. Vendor agrees to monitor and audit all access to and use of the Host Computer System and network. Access event activity logs for PHI will be maintained in a secure manner for a period of at least three (3) years. Other access event activity logs will be maintained for sixty (60) days. The access log will show, at a minimum, the date, time, data accessed, source IP address, and the identity of the user as to each event of access to data on the Host Computer System. The access log will be sortable, using commonly available

means, by date, user, and/or by the name of individual(s). Vendor will make the access log available to Trinity promptly upon its request for auditing and/or monitoring.

5. System Administrators.

a. General. Vendor shall have policies and procedures in place that govern its system administrator users' ability to access Trinity Data from the Host Computer System, with detailed controls for administrator passwords, user authentication, account management and data access, plus discipline and penalties for violations.

b. Minimum Number. Vendor agrees that Vendor will allow only the minimum number of system administrators to access and use the minimum necessary data to provide the Services.

c. Segregation of Duties. Vendor shall implement policies, processes and procedures to enforce and assure proper segregation of duties. In those events where a user-role conflict of interest constraint exists, technical controls shall be in place to mitigate any risks arising from unauthorized or unintentional modification or misuse of information assets.

d. Background Checks. Vendor shall require acceptable results from security background checks on all system administrator users of the Host Computer System.

6. Physical Security of Data and Remote Connectivity Centers.

a. Location. Vendor's data centers shall be housed in a United States location in secured areas, protected by a defined security perimeter, to protect Vendor's information processing facilities and the information in them from unauthorized access, theft, damage and environmental interference.

b. Facility Security. Vendor shall maintain a hosting environment that is physically secure to safeguard the Trinity Data and Vendor's information systems. This shall include, but not be limited to, fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols. Physical access to data and functions of users and support personnel shall be restricted. Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.

c. Access. Access to data centers and remote connectivity centers shall be physically restricted. Physical access protection may be achieved through physical barriers and entry identification controls.

d. Data in Transit. All Trinity Data shall be encrypted in transit. Industry recognized encryption includes SSL certificates of 256 bit strength or greater consistent with NIST & FIPS 140-2

Testing and Acceptance Exhibit

TESTING PROCESS

1. Test Plans. Vendor timely shall provide to Trinity its standard test plan, test scenarios and other similar materials for applicable Deliverables as specified in a Statement of Work and, if within the scope of Vendor's responsibilities under the applicable Order (or implementing document, such as a Statement of Work or Project Schedule), within the time frame specified in such Order (or implementing document), the parties jointly shall develop a final test plan (each, a "Test Plan") for testing the applicable ASP Services. Unless otherwise specified in the applicable Order (or implementing document), Trinity shall have primary responsibility for conducting the testing described in this Exhibit to verify and confirm that the ASP Services are successfully integrated and that they conform to, and perform in accordance with, the Documentation and SLAs. Due to the complexities inherent in the Testing Process, Trinity shall have the right to modify or amend the scope, methodologies and procedures for executing the Testing Process to include additional testing procedures and criteria if reasonably necessary to test the applicable ASP Services (and the applicable Test Plan shall be deemed modified accordingly).

2. Services Testing.

   a. Pre-Live Testing.
      i. Conversion Testing. Upon completion of all data conversions (if any) identified in the applicable Order (or implementing document), the responsible party (as specified in the applicable Order or implementing document) shall test the converted data in accordance with the applicable Test Plan to verify and confirm that such converted data can be fully reconciled with Trinity's original data. If within the scope of Vendor's responsibilities under the applicable Order (or implementing document), Vendor shall correct any identified discrepancies and errors in a timely manner or as reflected in the project schedule.
      ii. Functionality Testing and Correction of Defects. Pre-Live testing of the applicable ASP Services ("Pre-Live Testing") shall commence on the date specified in the project plan and shall test, as applicable: (a) the functional capabilities of the applicable ASP Services, (b) the information flows to and from the ASP Services, (c) the interfaces (including Custom Interfaces, if applicable), (d) the integration of the ASP Services with other Trinity systems, and (e) the transmission and processing of high-volume operational data in a production-simulated environment, all to verify and confirm that the ASP Services operate in accordance with the Performance Criteria.
   b. Live Testing.
      i. Live Testing Period. Following successful completion of Pre-Live Testing for the applicable ASP Services, Trinity shall have the number of days set forth in the project schedule (each, a "Live Testing Period") to conduct live testing of the ASP Services with actual data in order to verify and confirm that, as applicable: (a) the ASP

Services operate in accordance with the Performance Criteria, (b) the results generated by the ASP Services can be reconciled with the results achieved by operating Trinity's existing system, and (c) the ASP Services do not interfere with the performance of Trinity's other systems ("Live Testing"). If Trinity discovers any errors or discrepancies in the ASP Services during the applicable Live Testing Period, Trinity shall so notify Vendor, and Vendor shall correct such discrepancies and errors in accordance with the terms set forth in this Exhibit.

ii. Correction of Discrepancies and Errors. Upon Vendor's receipt of notice from Trinity during the applicable Live Testing Period of any discrepancies or errors, the Live Testing Period shall be suspended until Vendor corrects such discrepancies and errors. Vendor shall use its best efforts to correct such discrepancies and errors as expeditiously as possible and shall communicate with Trinity on an ongoing basis until the applicable discrepancy or error has been corrected. Upon Trinity's receipt of written notice from Vendor that such discrepancies and errors have been corrected, the Live Testing Period shall recommence; provided, however, that Trinity shall always have at least fifteen (15) days to verify any correction provided by Vendor. Without liming any other rights and remedies that may be available to Trinity, and without extending or otherwise affecting any time-based deadline, the process described in this Section shall repeat as often as necessary until all discrepancies and errors have been corrected, and Vendor shall perform its obligations relating thereto without additional cost or expense to Trinity.

3. Services Acceptance. "Acceptance" shall occur when Live Testing has been completed successfully for the applicable ASP Services and all Deliverables related to such ASP Services and required under the applicable Order have been provided to Trinity. Nothing else, including Trinity's use of the ASP Services, or any part thereof, in a live, operational environment, shall constitute Acceptance of any portion of the ASP Services. If Acceptance is not achieved for the applicable ASP Services within one hundred twenty (120) days after commencement of the Live Testing Period for such ASP Services, such failure shall constitute an Event of Default.

Support Services Exhibit

See attached Blackbaud CRM – Support and Maintenance description.

HIPAA Exhibit

See attached Business Associate Agreement.

Travel Policy Exhibit

See attached Travel Policy Exhibit.

Exhibit A

Blackbaud Hosting Service™

Service Description for Enterprise Clients

Services Purchased on Order Form

Blackbaud will provide applicable Application Hosting clients Hosting and/or Email Services, as stated and listed in the applicable Order Form.

Hosting Services Provided by Blackbaud

Provided your organization is current in its material obligations hereunder, Blackbaud will provide the following services ("Services"):

Installation: Blackbaud will install the hosted Blackbaud software on hardware with specifications that meet or exceed the system recommendations and third party compatibility information set forth in Blackbaud's Minimum System Requirements published at https://www.blackbaud.com/systemrequirements.

Access: Blackbaud will provide secure access to the latest supported version of hosted Blackbaud software via the Internet from a Hosting Services facility ("Hosting Site – Century Link with tape back-up") on a 24/7 basis (excluding Scheduled Maintenance as required). Scheduled Maintenance may be performed during the following Maintenance Windows, and Blackbaud will announce all planned upgrades and outages in advance as follows:

Maintenance Window	Windows Hours	Advance Notice
Standard Maintenance	Duration: Up to four (4) hours Time: Tuesdays and Thursdays 11:00 p.m. – 3:00 a.m. EDT/EST; Sundays 3:00 a.m. – 7:00 a.m. EDT/EST	No less than seventy-two (72) hours
Extended Maintenance	Duration: Up to nine (9) hours Time: Sundays 3:00 a.m. – 12:00 Noon EDT/EST	No less than thirty (30) days
Critical Maintenance	Duration: Up to two (2) hours Time: Nightly 10:00 p.m. – 12:00 Midnight EDT/EST	No less than one (1) hour

Maintenance Window start and end times may be amended with the same duration. Blackbaud will provide thirty (30) days advance notice to your organization of any such changes. Notifications of planned Scheduled

Exhibit A

Maintenance will be delivered to a designated point of contact via electronic mail. There may be instances of Emergency Maintenance where Blackbaud needs to interrupt the Services without notice in order to protect the integrity of the Services due to security issues, virus attacks, spam issues, or other unforeseen circumstances. Extended Maintenance Windows will be periodically scheduled for longer windows for application upgrades. Advance notice for these extended windows will be delivered to your organization so you may plan accordingly.

Availability: "Availability" means stable access to the production Services and access to the hosted software without substantial degradation to the Services such that the Services are unusable by your organization as a result of unreasonable response times. Blackbaud will provide 99.9% availability to the production Services calculated on a monthly basis, excluding Scheduled Maintenance (report provided upon request). If Blackbaud provides 99.7% or less availability in any given calendar month against the production environment, Blackbaud will credit you ten (10%) percent of the Hosting Services fee for the affected site(s) for such month. If Blackbaud provides 99.5% or less availability in any given calendar month against the production environment, Blackbaud will credit you twenty (20%) percent of the Hosting Services fee for the affected site(s) for such month. Availability calculations do not include Maintenance Windows. For any outage that crosses over a monthly boundary, that outage will be considered a single outage and the entire time window will be applied to the month's calculation in which the outage originated. The total available credit is 20%. To request a credit in the event that Blackbaud fails to meet the service level metrics, please notify Blackbaud in writing of both the date and the amount of time the services were unavailable within five (5) business days of the end of the month in which unavailability occurred. Blackbaud will research and confirm the information provided. If Blackbaud confirms that it did not meet the noted availability requirements, your organization will be credited based on the above availability credit definitions. Such credits will be applied to your organization's next invoice following the month in which the unavailability is confirmed.

Monitor: Blackbaud will monitor performance indicators on the systems and network infrastructure in order to gauge the overall performance of the Services, and will take reasonable steps to address systems and network infrastructure as required to maintain application performance. Blackbaud will use an internal system to measure whether the Services are available, and you agree that this system will be the sole basis for resolution of any dispute that may arise between your organization and Blackbaud regarding the availability of the Services.

Backup: Blackbaud will perform fully restorable data backups based on the following schedule:

Backup Type	Information	Retention	Location
Nightly	Incremental - digital	1 week	On-site
Weekly	Digital at alternate Centurylink location in Irvine CA	4 weeks	Off-site

Exhibit A

Monthly	Tape – Stored at Iron Mtn secure facility.	6 months	Off-site

You may request delivery of one (1) backup copy per month by creating a case with Support. Data backups stored off-site will be made available within five (5) days of the date of the retrieval request to Application Hosting Services Support. For an additional fee you may request that your backup be delivered to our secure FTP once per week, to be downloaded and used as your business needs demand.

Minor Upgrades and Patches: Blackbaud will install minor upgrades/releases of Application Hosting Services software, including patches and/or fixes, as they are made available to its general customer base at no charge. Blackbaud will determine and announce all planned upgrades as described in the Maintenance Windows section above. Through coordination with your TAM, your organization is required to be upgraded to the highest current minor version no less than twice per year. Delay or failure to upgrade on schedule may cause an increase in your fees to account for increased resources to maintain older versions. Refusal to upgrade may cause Blackbaud to terminate Services.

Major Upgrades: Upgrades to major releases (e.g., 6.x to 7.x) and related conversions require careful planning and data decisions that must be managed jointly by your organization and Blackbaud. Software installation of major releases will be performed by Blackbaud on a mutually agreed schedule not to exceed one (1) year after a major release of the software, provided your organization is a current maintenance customer. Additional services related to conversions to major releases (e.g., data conversion, report and software customizations, data cleanup, additional hardware) may be required and are outside the scope of the Services. Blackbaud will support the current version and one previous major version. Delay or failure to upgrade on schedule may cause an increase in your fees to account for increased resources to maintain older versions. Refusal to upgrade may cause Blackbaud to terminate Services.

Administrator: Blackbaud will provide your organization a single administrator user account for secure administrator access. Blackbaud will also make available to the administrator user tools to create other users for access to the Services.

Customizations: Blackbaud will support customizations built by Blackbaud Professional Services Developers which are built specifically for the Application Hosting Services environment. Client-built or third party-built customizations are not supported unless certified to be compliant with Blackbaud's development and security standards along with submitted DLL files in the Developers Guide. When applicable, customizations must be first deployed to staging for final validation, prior to promotion to production.

Non-production Environments

Blackbaud will provide optional "Non-Production Environment(s)" in addition to a Production Environment for Hosting Services, if specified in the Order Form. Non-Production Environments provide optional non-production system(s) and database instances on which to train staff and test or stage changes / configurations / customizations / integrations prior to promoting such changes to your production environment ("Production Environment"). "Development" Non-Production Environments provide access to an optional database instance on which to develop custom reports or develop customized software prior to promoting such customizations to Staging and then the Production Environment.

Non-Production Environment: Blackbaud will install Non-Production Environment(s) as specified in the Order Form running either the same version(s) of software installed in the Production Environment or, when applicable, upgraded to the proposed next release or patch supported by Hosting Services. During normal business hours (8:30am-6pm EDT/EST), your organization's data will be upgraded in a Non-Production environment to the proposed next release or patch once per software version release, and customizations installed for your evaluation prior to a production upgrade. Additional upgrades are available for an additional charge.

Each Non-Production Environment purchased on the Order Form will be accompanied by a single database instance.

Blackbaud will refresh your Non-Production Environment(s) upon request from the Production Environment, not to exceed more than one (1) request per month.

Your organization will have the same number of concurrent licenses available for each Non-Production Environment as are available for the Production Environment.

Development Non-Production Environment: Blackbaud will install a single Development Non-Production Environment, if specified in the Order Form, running the same version of software installed in the Production Environment.

Blackbaud will refresh your Development Non-Production Environment upon request from the Production Environment, not to exceed more than one (1) request per month.

All development must be done in accordance with Blackbaud's published Application Program Interfaces.

Blackbaud reserves the right to review the Functional Specification and code of all customizations developed by, or on behalf of, your organization, and has the right to reject such specifications or code based on the findings that the specification or code may cause detrimental harm to the Application Hosting Services, or does not meet Blackbaud's compliance requirements including OWASP Top 10, SANS Top 25, and PCI DSS.

Blackbaud and your organization may coordinate a Quality Assurance and Performance Impact Test, and Blackbaud and your organization will approve, in writing, the deployment of SQL or Custom Code into either the Non-Production Environments or Production Environments.

Upon approval, SQL statements and custom code developed by your organization will be loaded into the Non-Production Environments or Production Environment on a schedule as agreed between your organization and Blackbaud, not to exceed five (5) business days.

PCI-DSS: In compliance with Payment Card Industry-Data Security Standards (PCI-DSS), the Non-Production Environments are not allowed to test a live Primary Account Number (PAN). Testing must be done using either the "test" or "demo" mode of your merchant account. For more information on these modes, please review the Administrators Guide for your specific Blackbaud application. For example, please see page 66 in the following guide: https://www.blackbaud.com/files/support/guides/bbnc/adminec.pdf.

Access: Blackbaud will provide secure access to all Non-Production Environments with the latest supported version of hosted Blackbaud software via the Internet from a Hosting Services facility ("Hosting Site") on a 24/7 basis (excluding Scheduled Maintenance as required). Non-Production Scheduled Maintenance may be performed during the same Maintenance Windows as Production.

Availability: "Non-Production availability" means stable access to the Non-Production Services and Non-Production hosted software without substantial degradation to the Non-Production Services such that the Non-Production Services are unusable by your organization as a result of unreasonable response times. Blackbaud will provide 99.0% availability to the Non-Production Services calculated on a monthly basis, except for scheduled and emergency maintenance. Service level credits will not be available for non-production environments.

Backups: Blackbaud will NOT perform ANY backups in the Non-Production Environments, with the exception of a training master copy, where applicable.

Customizations: Blackbaud will install customizations into the Non-Production Environments provided that (a) the Functional Specifications of all customizations developed by your organization or Blackbaud have been approved by Blackbaud Application Hosting, and (b) certified to be compliant with Blackbaud's development and security standards. Customizations developed by your organization will be loaded into the Non-Production Environments within five (5) business days of the Support request.

Email Services Provided by Blackbaud

Provided your organization is current in its material obligations hereunder, Blackbaud will provide the following services if listed on the applicable Order Form:

- **Bulk Email Service:** Bulk email is defined as an email message that is sent to one or more recipients at a time specified by your organization. Examples of bulk email include, but are not limited to, newsletters and blasts. Must follow state and spam laws.
- **Transactional Email Service:** Transactional email is defined as an email message that is sent to one recipient in response to an action initiated by the recipient. Examples of transactional email include, but are not limited to, donation acknowledgements, opt-in confirmations, and event registration confirmations.
- **Email Forwarding Service:** Email Forwarding is defined as reception of email to an email address hosted by Blackbaud and automatically forwarding it to a different email address as specified by your organization or one of your organization's constituents. An example of Email Forwarding is where email sent to JohnSmith@alumni.university.edu is received by Blackbaud and forwarded to JohnSmith@hotmail.com.
- **Domain Name Service (DNS) Configuration and Maintenance:** Blackbaud will configure and maintain all necessary DNS records to ensure proper delivery of email through Services. Blackbaud will only configure and maintain DNS records for those domains exclusively used for Blackbaud Internet Solutions.
- **Blacklist Monitoring:** Blackbaud will monitor all private and shared IP addresses used for Email Services for inclusion on any of the well-known Blacklists. When an IP address is listed on any of the well-known Blacklists, Blackbaud will take appropriate action to get the IP address removed from the Blacklist.

Your Responsibilities

Your organization is responsible for the following:

Maintenance: Purchase and remain current in one of Blackbaud's maintenance and support programs.

Primary Contact: Identify an appropriate individual as primary contact with whom Blackbaud should communicate matters regarding the Services, such as maintenance notifications and who has the authority to make Services requests including restoration of data, configuration changes, and release of your organization's data, both to Blackbaud and internally to your organization.

System Requirements: Review all applicable system requirements and recommendations for the Services purchased.

Administering Security: Security administration within the Blackbaud software (e.g., the granting of rights to a user for a specific form in the application). Your organization is also responsible for maintaining its user desktops and providing users with network access to the Services.

Connectivity: Provide connectivity and security to the Internet for its location(s) for purposes of providing adequate access to Services at the Hosting Site. Blackbaud will not be responsible for the reliability, performance or continued availability of the communications lines, or the corresponding security configurations used by your organization in accessing the Internet to access Services.

Integration Between Your Site and Blackbaud: Follow industry standard security methods for any integration between applications at your organization's site and Services hosted by Blackbaud.

Operational Changes: Advise Blackbaud of any changes to your organization's operations, banking relationships, primary contact, or other information that would require a change in the support, operation, or configuration of the hosted applications.

BBPS: Separate Agreement. Establish an account with Blackbaud Payment Services™ for credit card transactions, if applicable.

Email Services:

- Delegate to Blackbaud the authority to manage DNS configuration for email domains used by Services, except where your organization chooses to use an email domain provided by Blackbaud.
- Do not send unsolicited commercial email (UCE).
- Do not send commercial email to an individual's email address unless your organization has the prior affirmative consent of the individual to do so (as that term is defined under U.S. Law within CAN-SPAM), or has obtained the prior consent of the individual in a manner compliant with the European Commission Privacy and Electronic Communications Directive.
- Every Bulk Email that your organization sends must include an opportunity for the recipient to unsubscribe from receiving such email in the future.
- Process requests to unsubscribe within three (3) business days, and inform the recipient of the length of time required for processing.
- Do not gather email addresses using surreptitious methods (e.g., scraping or harvesting).
- Notify Blackbaud NetCommunity™ support via email five (5) business days in advance of when there will be any changes to your organization's Mail Constructor Service server IP address to coordinate the IP address transition date and time.
- Use all email domains and sub-domains owned by your organization but configured for use for Blackbaud NetCommunity email services exclusively for Blackbaud NetCommunity.

Service Use Restrictions

Email forwarding web services may not be used for bulk transfers of mail from any source; the Services are intended for individual users only. Your organization may not lease its capacity for use by third parties. Your

Exhibit A

organization may not use the Services to take any actions that (i) infringe on any third party's copyright, patent, trademark, trade secret, or other proprietary rights or rights of publicity or privacy; (ii) violate any applicable law, statute, ordinance, or regulation (including those regarding export control); (iii) are defamatory, trade libelous, threatening, harassing, or obscene; (iv) interfere with or disrupt network users, services, or equipment with the intent to cause an excessive or disproportionate load on Blackbaud's or its suppliers' infrastructure by means of (but not limited to) distribution of unsolicited bulk emails or chain letters, viruses, Trojan horses, worms, or other similar harmful or deleterious programming routines; or (v) constitute unauthorized entry to any machine accessible via the network. Your organization will be subject to the usage policies of Blackbaud's third party service providers. These use restrictions are subject to change upon thirty (30) days prior notice to your organization.

Storage Space

A default maximum of storage space, including the backup and off-site storage and tape retention thereof, is available for your organization within the Application Hosting Services. The default maximum storage space will be the greater of the number listed below or the storage number specified in the applicable Order Form. The default maximum storage calculation will be based on the production database size. Blackbaud will monitor disk usage on a regular basis, and will increase your organization's disk space allocation per the price schedule in the Order Form, when disk utilization exceeds the next pending threshold.

Hosted Application	Default Maximum Storage Space
Blackbaud CRM™ Blackbaud Direct Marketing™	9 TB
Team Approach®	120 GB
The Raiser's Edge®	10 GB
Blackbaud NetCommunity™	5 GB
The Patron Edge® Online	5 GB
The Financial Edge™	5 GB
The Education Edge™ Blackbaud Student Information System™	5 GB
The Researcher's Edge™	1 GB

Exhibit A

Altru	20GB
PaperSave®	20 GB
Advanced Budget Management	5GB
Files Folder	100 MB per user

Termination

For Clients with hosted Software: The Parties may mutually agree to terminate Client's Hosting subscription. In the event of any such mutually agreed termination, Blackbaud shall provide Client with a copy of the Software source code along with a copy of Client's database in an industry standard format.

Changes to this Service Description

The terms of this Service Description are subject to change in Blackbaud's sole discretion. In the event of any such change, Blackbaud will post a revision of this Service Description at www.blackbaud.com and notify the client in writing.

To learn more about Blackbaud Hosting Services™, visit www.blackbaud.com or contact your Blackbaud account representative.

Exhibit A

blackbaud
your passion ▸ our purpose

Blackbaud CRM™ – Support and Maintenance

Definitions

- **Account Review Sessions** means regularly scheduled sessions for Blackbaud and Client to review recent and open Support Services and Maintenance Services cases and address other open issues.
- **Approved Modification** means a modification to the Covered Software made by or on behalf of Client using the Tools or made by Blackbaud at Client's request.
- **ATP** means an Agreement to Purchase issued pursuant to this Agreement.
- **Covered Software** means the Software, Tools, and Upgrades together.
- **Covered Technology** means the Covered Software and the Approved Modifications together.
- **Errors** means errors, including those related to data, in the Covered Technology that interfere with Client's critical business processes.
- **Extensibility Features** means other extensibility tools to be used beyond the Software Developer Kit (SDK).
- **License** means the terms of the license for the Software and the Tools, as set forth in the Agreement.
- **Maintenance Services** means the Services provided to Client pursuant to their purchase of a Blackbaud maintenance program.
- **Major Release** means the version of the Covered Software reflected by the numerical value to the left of the decimal point in the version number.
- **Planned Obsolescence** means a period during which Blackbaud no longer markets, supports, or maintains the Covered Software.
- **Platform** means the common platform on which the Software is built.
- **Point Release** means the version of the Covered Software reflected by the numerical value to the right of the decimal point in the version number.
- **SDK** means certain proprietary software extensibility tools, commonly defined as the Software Developer Kit.
- **Software** means the Blackbaud software purchased by Client pursuant to an Agreement to Purchase (ATP).
- **Supplemental Maintenance Services** means additional maintenance services provided by Blackbaud at Client's request and for additional fees, as more particularly described in Supplemental Maintenance Services below.
- **Support Report Card** means the written Support Services and Maintenance Services report card provided to Client.
- **Support Services** means the Covered Software-related Support Services provided to Client as more particularly described in Scope of Support Services, below.
- **Support Team** means the Blackbaud support team providing Support Services to Client.
- **TAM** means a Technical Account Manager provided by Blackbaud pursuant to Client's purchase of an annual TAM subscription.

- **Technical Contacts** shall mean Client's designated internal support resource serving as the key liaisons between Client and the Support Team for technical support of programs and use of Maintenance Services and Support Services.
- **Tools** means the SDK and Extensibility Features together.
- **Upgrades** means new releases, versions, updates, upgrades, patches, and enhancements to the Covered Software.
- **Unapproved Modification** means a modification using the Tools or any other method of Extensibility Features that alters or deletes any Platform entities (including, but not limited to: tables, columns, xml files, or CRL code) and is not an approved or supported alteration.

Blackbaud Maintenance Services

Software Upgrades. Blackbaud will provide Upgrades as they become available. Such Upgrades will be treated as Covered Software under the License. Some new versions, updates, or enhancements may require more advanced or larger capacity equipment, or third party software, compatibility with which shall be sole responsibility of Client in these circumstances for Covered Technology not hosted by Blackbaud. Blackbaud's Support website is the primary means of communicating information about Covered Software and Upgrades. Blackbaud will provide detailed specifications about Upgrades as reasonably requested by Client to enable Client to meet Client obligations under this section. Blackbaud will provide modified documentation in connection with such Upgrades, as applicable.

Correction of Software Errors. Blackbaud will use commercially reasonable efforts to correct Errors in the Covered Software. Blackbaud's obligations in this section may be limited due to the version of the Covered Software being used by Client, as further detailed in Supplemental Maintenance Services.

Correction of Data Errors. Blackbaud will use commercially reasonable efforts to correct data-related Errors that are directly attributable to programming in the Covered Technology. Blackbaud's obligations in this section are dependent on Client's performance of scheduled data backups for Covered Technology not hosted by Blackbaud and use of best practices in data processes. Limitations on the correction of data-related Errors are covered in Supplemental Maintenance Services.

Exclusion from Maintenance Services. Blackbaud will not correct Errors arising from Unapproved Modifications.

Supplemental Maintenance Services

Examples of Supplemental Maintenance Services include:

- Provision, installation, or support of new versions or enhancements to non-Blackbaud software on non-Blackbaud infrastructure. Non-Blackbaud software includes but shall not be limited to, operating system software, word processing, spreadsheet, reporting, or database software.
- Upgrading any hardware and memory on the system on which Client uses the Covered Technology.
- Repair of the Covered Technology and Errors or loss if Blackbaud determines the needed repair is related to:
    - Client using equipment or supplies other than those required by Blackbaud in the documentation for running the Covered Technology.

- Misuse or neglect of the Covered Technology including, but not limited to, failure to perform scheduled data backups using a prudent method of media rotation for Covered Technology not hosted by Blackbaud.
- Environmental conditions for Covered Technology not hosted by Blackbaud, including, but not limited to, insufficient, excessive, or irregular electrical power, failure of air conditioning, excessive heat or humidity, flood, water, wind, or lightning .
- Use of the Covered Technology for purposes other than those for which it was expressly designed.
- The relocation or reinstallation of the Covered Technology not hosted by Blackbaud, although Blackbaud will provide support without supplemental charges after the relocation or reinstallation activities by Client are completed.

- Upgrade testing for the purposes of testing compatibility of specific Approved Modifications or specific Client business processes. However, resolution of issues with Approved Modifications associated with Upgrades is as detailed in Support and Maintenance for Approved Modifications, below.
- Installation of Upgrades to the Covered Software on Client infrastructure.
- Implementation of new software functionality or conversion of data from customizations into new software functionality of the Covered Software.
- Changes to Approved Modifications to meet government or industry regulations.

Blackbaud reserves the right to limit the scope of the Maintenance Services and Support Services provided to Client if the production version of the Covered Software is not within one (1) Major Release of the current version.

Blackbaud reserves the right to limit the scope of the correction of software defects to Client if the production version of the Covered Software is not within two (2) Point Releases of the current version.

Scope of Support Services

Support Services, including those described in Exhibit A, include:

- Unlimited online and telephone consultation to assist Client with use of the Covered Software.
- Providing a new features guide for description of new functionality in each Major Release or Point Release.
- Diagnosing problems, issues, or Errors with respect to the Covered Software.
- Using commercially reasonable efforts to resolve reported and verifiable Errors in Covered Technology.
- Answering questions about and troubleshooting the installation or upgrades of the Covered Software.
- Offering direction on troubleshooting performance issues.
- Assisting with the use of Blackbaud-created troubleshooting tools.
- Offering direction in setting up users and system roles.
- Offering guidance in troubleshooting users and system roles.
- Offering direction regarding setting up Key Performance Indicators ("KPI"), Smart Fields, and Selections.
- Assistance with Approved Modifications that may be affected by Upgrades, as defined in Support and Maintenance for Approved Modifications.
- Developer assistance with Approved Modifications using the Tools with an annual SDK subscription as described in the SDK Support section below.

Unless otherwise required in a Blackbaud-hosted environment, Support Services do not include:

- Troubleshooting Citrix, VPN or any other remote connections to the Covered Software. NOTE: Machines should be on the same domain as the web server or the application should be published publicly.
- Troubleshooting software issues that can only be duplicated through a remote connection.
- Firewall configuration or troubleshooting.
- Resolving issues with IIS.
- Setting up SSL certificates.
- Configuration of printer hardware.
- Configuration of SQL Server reporting service.
- Load balancing hardware/software (such as NetScaler).
- Software or technical training.

SDK Support

Provided that Client purchases an annual SDK subscription, Blackbaud will provide Support Services for SDK as described herein. By providing written notice to Blackbaud, Client may increase or decrease its desired number of SDK users, and shall be responsible for any fees associated therewith. Blackbaud strongly encourages the use of the SDK when developing Approved Modifications.

The following documentation is provided with the Covered Software:

- Complete data dictionary/database schema documentation in hypertext help format.
  - Version comparison documentation, Search feature, Copy code functionality, Intellisense, and documentation when authoring catalogue specifications.
- Documentation for previously released versions.
- Reference assemblies.
  - Blackbaud.AppFx.Server.dll, Blackbaud.AppFx.Browser.exe, Blackbaud.AppFx.Controls.dll, Blackbaud.AppFx.XmlTypes.dll, Blackbaud.AppFx.WebAPI.dll.
- Sample code that illustrates calling Blackbaud's web service API code.
  - Widgets, Web API sample, Linux/Apache (.php) demo files, Adobe Flex (Flash), VBScript demo.

SDK Support Services include:

- Explanation of the concepts and theories behind Blackbaud extensibility, which includes:
  - Providing guidance and direction on best practices of the Extensibility Features.
  - Discussing and evaluate possibilities for custom creation that works best with the Client's database structure and business processes.
  - Loading and deployment of catalog specs. Note: Client developers must be aware of the status of catalog specs that have been deployed.
  - Assisting in diagnosing issues in Client-created custom parts.
  - Explanation of functionality when creating custom report specification.

  - Using referenced Blackbaud Enterprise programming elements.
  - Examples in Visual Basic 2008.
- Explanation of the concepts and theories behind Blackbaud database structure, which includes:
  - Relationships between Blackbaud-created tables and fields.
  - Blackbaud-created and maintained database objects within the Blackbaud Enterprise database.
  - Providing guidance and direction on best practices for Blackbaud Enterprise database development.
  - Verification of connectivity to database using an ODBC connection.
  - T-SQL compliant examples.
- Explanation of concepts and theories behind using Microsoft SQL Server Report Writing Services 2005 and 2008 to create custom reports, which includes:
  - Troubleshooting expressions, variables, and parameters created using Visual Basic 2005\2008 syntax.
  - Deploying reports within the Covered Software using the SDK.
  - Providing guidance and direction on best practices for Blackbaud Enterprise custom report development.
  - Accessing data from Blackbaud-created databases.
  - Assisting with creating and troubleshooting data sources and datasets.
  - Assisting with formats and display of data from Blackbaud-created databases extraction.

Supplemental Maintenance Services for SDK are available for the following items, as they are outside the scope of SDK Support Services:

- Installing or troubleshooting SQL Server issues.
- Training or instruction on programming languages.
- Providing consulting or project management work.
- Creation, installation, administration and usage of custom assemblies in a report.
- Using SQL Server 2005 & 2008 Report Manager and Report Server Web Service outside the context of the SDK-specific report catalog item.
- Providing fully-functioning standalone solutions.
- Rewriting code in order to return a completed Approved Modification.
- Providing fully-functioning standalone reports.
- Answering questions regarding specifications, features, intended usage, and the operation of Client-developed customizations, including reports.

Client's contacts for SDK Support Services are recommended to have the following skills:

- Fluent in any .NET language.
- Experience with Microsoft SQL Server 2008.
- Experience with reading, authoring, and editing XML documents.
- Experience working with Microsoft SQL Server Reporting Services.

- Experience with design and implementation of relational databases including using transact SQL to build stored procedures and user defined functions.
- Experience designing and building reports on the Microsoft Reporting Services platform.

Non-Blackbaud developers working on Client's behalf should have the following knowledge of the Covered Software:

- Customization knowledge including, but not limited to, creating a new table, table extension, data list, data form, data view form, output format files, custom business rules, rule base constituency codes, database schema, and using the catalog browser.
- Core product knowledge including, but not limited to, CRM and related modules, administrative functions, and page designer.
- Implementation knowledge including, but not limited to, Client and site specific business practices, configuration, and policy and procedures. Blackbaud highly recommends SDK developers remain involved during scope and implementation of the Covered Software.

Support and Maintenance for Approved Modifications

Approved Modifications will continue to operate with Upgrades and neither Approved Modifications nor Upgrades will materially degrade the functionality of the Covered Technology.

Any Unapproved Modification, including any modifications to any third party licensor software included with or embedded in the Covered Software, will void Blackbaud's maintenance and warranty obligations with respect to the affected component of the Covered Technology.

Client is fully liable and responsible for all Unapproved Modifications and any errors or damages resulting from such Unapproved Modifications. If Client successfully reverses an Unapproved Modification, as acknowledged in writing by Blackbaud (which acknowledgment shall not be unreasonably withheld), Blackbaud's maintenance and warranty obligations hereunder with respect to the affected components shall re-commence.

If a Blackbaud-developed Approved Modification contains an Error due to an Upgrade, Blackbaud will use commercially reasonable efforts to correct such Error(s) in the Approved Modification until such time that a Planned Obsolescence has been declared on the Covered Software or parts of the Covered Software affecting any Approved Modification. In addition to this, Blackbaud will assist the Client with any reasonable questions related to their Approved Modification should it break as part of an Upgrade, until such time that a Planned Obsolescence has been declared on the Covered Software or parts of the Covered Software affecting any Approved Modification. Any other questions about troubleshooting, changing or creating Approved Modifications would be contingent on the status of the Client's SDK subscription.

Continuing Support for Covered Software and Approved Modifications; No Planned Obsolescence Until After Three-Year Anniversary

Blackbaud agrees to support and maintain the Covered Software for at least three (3) years from the ATP Effective Date or until a Planned Obsolescence.

Blackbaud will provide Support Services for Approved Modifications and reports created by either Blackbaud or Client or on behalf of Client until a Planned Obsolescence occurs, in accordance with this section.

Blackbaud will not declare a Planned Obsolescence for the Covered Software to take effect any earlier than three (3) full years after the Effective Date (the "Three Year Anniversary").

If Blackbaud decides to effect a Planned Obsolescence after the Three Year Anniversary, Blackbaud will provide Client as much advance written notice as possible of the Planned Obsolescence effective date (the "Planned Obsolescence Effective Date"), but in no event will Blackbaud effect a Planned Obsolescence earlier than one (1) year after notice given to Client of the Planned Obsolescence Effective Date.

Technical Account Manager

Provided that Client purchases an annual TAM subscription, Blackbaud will provide Support Services for TAM as described herein.

The Technical Account Manager shall:

- Coordinate the efforts of the Support Team on behalf of Client.
- Oversee Client support requests, conduct Account Review Sessions, and monitor the interaction of Blackbaud staff with Technical Contacts.
- Serve as one of the points of issue escalation when appropriate.
- Disseminate any relevant information and situations to the Support Team and Blackbaud management as appropriate.

If Client requests replacement of the TAM, Blackbaud will use commercially reasonable efforts to assign a different TAM who is reasonably acceptable to Client, at no additional cost. While the TAM is the primary contact for Client with the Support Team, the entire Support Team will work with Client as needed to provide timely assistance.

Based on a mutually agreed schedule, the TAM will conduct the Account Review Sessions. Following these session, the TAM will provide Client with a Support Report Card.

In addition to other details to be included by mutual agreement of Client and the TAM, the Support Report Card will include:

- Cases or issues closed within the agreed upon time frame.
- Open cases or issues and current action plans.
- Proactive notification of new product functionality, including new features guide.
- Clear communication of action items and next steps.

Internal Support and Technical Contacts

Client shall assign up to six (6) Technical Contacts. Blackbaud recommends that Client designate at least two (2) Technical Contacts. To avoid interruptions in the Maintenance Services and Support Services, Client agrees to notify Blackbaud whenever Technical Contact responsibilities are transferred to another individual. In the event of

blackbaud
your passion > our purpose

Technical Contact staff turnover and to ensure appropriate execution of Technical Contact responsibilities, Client is required to provide training to all Technical Contacts within 90 days of a new Technical Contact being designated. Training shall include, at a minimum, Blackbaud troubleshooting practices, functionality of the Covered Software and internal business practices, and all such training to be provided at Client's expense.

Client retains the responsibility for providing internal support for the Covered Technology, including:

- Responding to internal users with respect to inquiries concerning the performance, general or complex functionality, or operation of the Covered Technology.
- Responding to internal users with respect to Errors or issues with the Covered Technology.
- Diagnosing Errors or issues with Covered Technology.
- Resolving Errors or issues with the Covered Technology.

If after using reasonable efforts Client is unable to diagnose or resolve Errors or issues of the Covered Technology, Technical Contacts may contact the Support Team. Technical Contacts will be required to provide the Support Team information and access to applicable software systems including access to Client repository files, log files, database extracts, and database, as necessary for Blackbaud to provide Support Services and Maintenance Services. In the event Client fails to provide Blackbaud the necessary information and access, then Blackbaud will use commercially reasonable efforts to perform the Support Services and Maintenance Services, but such Services may be limited in proportion to such limitation on information and access. Blackbaud will use commercially reasonable efforts to provide Client general guidance on use of the Covered Technology and general guidelines on regarding the information Technical Contacts should provide when contacting the Support Team.

Client must have qualified SQL Server 2008 or later Database Administrator to perform regularly required administrative tasks. Assistance provided by Blackbaud with SQL 2008 or later administrative operations is considered a Supplemental Maintenance Service.

EXHIBIT A – Support Services Detail

This Exhibit A details the availability and management of Support Services. All references to SDK or TAM in this Exhibit A apply only to the extent that Client has an active and paid subscription for such services. The terms of this Exhibit A are subject to change in Blackbaud's sole discretion. In the event of any such change Blackbaud will post a revision of this Exhibit A at www.blackbaud.com and notify the client in writing.

Support Definitions

- **After Hours Support** means support provided outside of Normal Support Hours.
- **All Other Issues** means:
  - **Problem**: The Error causes only a minor impact on Client's use of the Covered Software, including, without limitation, partial loss of service to an individual(s) within a department.
  - **Noncritical/Question**: General how–to question on functionality or product. Although an Error exists, it does not impact the operation of the Covered Software. The Error causes minor inconveniences such as cosmetic problems or is a User Documentation inaccuracy.

  - **Suggestion:** Covered Software works as designed but new functionality or change in process is requested by Client.
- **Commorcially Reasonable Workaround** means alternative programmatic steps or environmental changes that achieve the end goal of the Covered Software function.
- **Critical** means (a) the issue requires immediate attention and (b) no Commercially Reasonable Workaround exists and (c) a critical business process or major feature is failing that prevents acceptance of live donor transactions.
- **Down** means that Client (or large subsection of Client) is unable to access or login into the database or a Blackbaud-hosted environment.
- **Final Resolution** means any programmatic or design changes, usually accomplished through a patch or version release, that resolve the root cause of Covered Software Errors.
- **Normal Support Hours** means 8:30 a.m. – 8:00 p.m. EST/EDT (Monday – Thursday) and 9:00 a.m. – 8:00 p.m. EST/EDT (Friday), excluding holidays.

Support Team

Blackbaud provides support for All Other Issues during Normal Support Hours.

Blackbaud provides support for Down and Critical issues on twenty-four (24) hours per day, seven (7) days per week, three hundred sixty-five (365) days per year basis.

The Support Team can be reached in any of the following ways:

- Online: www.support.blackbaud.com
- Case Central: casecentral.blackbaud.com
- Email (by product)
  - Blackbaud CRM™: besupport@blackbaud.com
  - Blackbaud NetCommunity™: bbncsupport@blackbaud.com
  - Software Developer Toolkit (SDK): sdksupport@blackbaud.com
  - Support & Maintenance Services: maintenance@blackbaud.com
- Phone: 1.800.468.8996 (enter site ID or case number at the prompt).
- Fax: 1.843.216.6100.
- Direct contact with the TAM or the secondary TAM substitute, provided that the TAM shall have acknowledged receipt of the contact.

For After Hours Support for Critical or Down issues please use one of the following methods:

- Email (by product)
  - Blackbaud CRM: besupport@blackbaud.com
  - Blackbaud NetCommunity: bbncsupport@blackbaud.com
  - Software Developer Toolkit (SDK): sdksupport@blackbaud.com
  - Phone: 1.800.468.8996 (enter site ID at the prompt).

blackbaud
your passion > our purpose

Escalation and Resolution Times

Blackbaud will provide an initial response to Client requests for support as soon as possible. Responses will be provided no later than sixty (60) minutes of receipt of original request. Blackbaud aims to answer all incoming calls within four (4) minutes and provide initial responses to email requests within twenty (20) minutes.

Critical or Down issues will be addressed to provide either a Commercially Reasonable Workaround or Final Resolution as promptly as possible. All issues that are not resolved on the first contact will be monitored by TAM for Client and evaluated by Client and key Blackbaud resources to prioritize and focus top attention on those issues adversely affecting Client. All Other Issues will be evaluated on a case-by-case basis and prioritized according to the nature of the issue.

Client acknowledges that resolving software issues is a collaborative effort between Client and Blackbaud. Resolving software issues is often complex and may involve variables unrelated to Support Services, including third parties, expertise and responsiveness of Technical Contacts, and access to client data, which may adversely impact resolution and response times.

Cases will not be downgraded or marked as resolved until either: a Commercially Reasonable Workaround is provided that corrects the reported Error, a Final Resolution is provided, or a solution is provided as mutually agreed by Blackbaud and Client.

TRAVEL AND BUSINESS EXPENSE POLICY EXHIBIT

Actual Costs: All travel and living expenses are billed for actual costs incurred, with the exception of the per diem meal allowance. Receipts are retained for all expenses.

Airfare: Airfare is the cost of round trip coach fare according to the following rules:

1. If travel originates and ends at the same location, Trinity Health pays the total fare. If travel is between client sites, Trinity Health will pay the fare only for the segment(s) between last client site and Trinity Health. For example, if a consultant flies from the consultant's home airport to client A in Chicago ($175) then from Chicago to a Trinity Health site in Michigan ($250), then CHE Trinity Health's obligation will be for the fare between Chicago and Michigan ($250).

2. Reservations and ticketing are made as early as possible, using discounted, advance bookings, in order to obtain the lowest possible fare. Trinity Health assumes the risk for penalties due to cancellations as a result of Trinity Health Affiliate's changes in consultants' schedules. Supplier assumes the risk for penalties arising from Supplier-requested schedule changes.

Lodging and Meals

1. Lodging: Lodging is acquired near Trinity Health Affiliate's offices at a price agreeable to Trinity Health and consistent with area rates. Suppliers use Trinity Health's corporate rate at designated hotels whenever possible.

2. Per Diem: Meals - Meal expenses are calculated on a per diem basis, including all meals, tips, and incidental expenses. The per diem amount varies based on the city and county in accordance with GSA guidelines.

Transportation

1. Car Rental: Car rental is for a four-door intermediate when there is more than one passenger. Suppliers attempt to share transportation if possible.

2. Taxis/Trains: Trinity Health is billed for the cost of taxi, bus, shuttle, or train fare to Trinity Health Affiliate's offices. Suppliers attempt to use the most cost and time efficient means for commuting to Trinity Health Affiliate's site.

3. Parking/Tolls: Trinity Health is billed for the cost of parking and tolls associated with transportation to Trinity Health Affiliate's site, as well as airport parking and mileage to and from the airport.

4. Mileage: Mileage is billed at the standard rate published by the IRS and in accordance with the following rules:

5. Local - The lesser of the round trip distance from the Supplier's office to the Trinity Health Affiliate site or the round trip distance from the Supplier's home to the Trinity Health Affiliate site.

Travel and Business Expenses

It is the policy of Trinity Health that all travel and business expenses be properly authorized, reported and reimbursed. It is the responsibility of Supplier and/or Supplier worker to accurately report their travel expenses in accordance with the guidelines set forth below. It is the responsibility of the Trinity Health manager authorized to approve travel expenses to review each expense report to ensure it is consistent with the guidelines below. Trinity Health management staff may approve exceptions to the guidelines if sound business reasons warrant.

Authorization. When possible, all travel and business expenses are to be pre-approved the appropriate Trinity Health manager. Supplier will make its best effort for travel and business expenses to be pre-approved by the Trinity Health manager.

Expense Report. Travel costs will be invoiced to Trinity Health by Blackbaud. Receipts are required and will be provided to Trinity Health for all expenses equal to or greater than $25. If not clearly evident, the business purpose for the travel and/or business expense should be documented. These written reports are required by IRS guidelines.

Air Travel. All reservations should be made as far in advance of the travel date as is reasonable and appropriate. The lowest possible rate, irrespective of carrier, is expected.

Class of Service. All Suppliers and/or Supplier workers are expected to travel coach class on Trinity Health business. All Suppliers and/or Supplier workers travel by air are expected to plan their trips utilizing the lowest logical airfare.

Excess Baggage. Supplier personnel on Trinity Health business are each permitted two pieces of baggage wherein airline baggage charges are reimbursable. Personal baggage exceeding two bags is not reimbursable, although excess baggage charges for company materials are reimbursable.

Air Travel vs. Automobile Travel. Air travel should not be used for destinations that are two (2) hours or less driving time away from Supplier and/or Supplier workers' base office.

Travel Time. Supplier will be responsible for costs related to Supplier's travel time to its Trinity Health business locations, if any.

Airport Connections. The least expensive alternative (i.e., , non-charter airport limousine service, rental car, cab) for travel to and from airports should be used
Airport Parking. Use of parking lots is reimbursable.

Automobile Rental. Use of automobile rental is highly discouraged if there is a less expensive alternative available.

Automobile Class. A compact car should be reserved when there is one passenger. A mid-size/intermediate car may be reserved when there are two or more passengers.

Incidental Expenses. Expense for tolls, parking and refueling are reimbursable. Traffic tickets or fines associated with traffic violations, including parking are the responsibility of Supplier.

Hotels. Supplier and/or Supplier workers are expected to use properties with which Trinity Health has established a preferred rate program or a Blackbaud Preferred Rate if lower than Trinity Health's preferred rate program. The Trinity Health manager can supply Supplier with the latest list of preferred hotels.

Room Service, In Room Bar/Snack Service. Room services and in room bar/snack service may be utilized and should be recorded on the expense report as reimbursable meal expense. It is expected that this expense would remain consistent with meal reimbursement guidelines.

Laundry/Valet Service, Movies, Sports, Health Club and Activity Fees. Laundry, valet, movies, sports, health club and activity fees are not a reimbursable expense.

Tipping. Tips are reimbursable and generally should be limited to: (i) baggage handling, $1 per bag; (ii) maid service, $1 per day; and restaurant, 15% to 20% of meal cost. Tips should be itemized on expense report.
Meals. Trinity Health will reimburse for meals pier diem based on GSA guidelines. Supplier and Supplier workers will be reimbursed for meals only in those situations when an overnight stay away of Supplier and/or Supplier's home is required by Trinity Health.

Saturday Night Stay. Often there is a significant reduction in the cost of airfare if the itinerary includes a Saturday night stay. In such instances, Trinity Health will cover the cost of the additional hotel expense up to the amount of the airfare savings.

Trinity Health

Professional Services Statement of Work

Prepared by Susan U. McLaughlin, CFRE

April 10, 2015

blackbaud
your passion > our purpose

Exhibit A

Version Control Log

Date	Name	Description	Sections	Rev.
04/10/15	Susan McLaughlin	Internal – Initial Creation	All	
05/11/15	Susan McLaughlin	Initial Review with Client	All	1.0

Table of Contents

1 **EXECUTIVE SUMMARY** **3**
- 1.1 Project Overview 3
- 1.2 Solution Overview 4
- 1.3 Project Approach 5

2 **PHASES AND DELIVERABLES** **7**
- 2.1 Responsibility Matrix 7
- 2.2 Group 1 Deliverables 7
- 2.3 Groups 2 through 4 Deliverables 17

3 **ASSUMPTIONS & CLIENT RESPONSIBILITIES** **20**
- 3.1 General Assumptions & Responsibilities 20
- 3.2 SOW Specific Assumptions & Responsibilities 22

4 **FEES, BILLING AND CHANGE ORDERS** **27**
- 4.1 Estimated Services 27
- 4.2 Billing Terms 27
- 4.3 Implementation Pre-Payment 27
- 4.4 Change Orders 28
- 4.5 Expiration of Services 28
- 4.6 Cancellation Policy 28

5 **SOLUTION SPECIFIC COMPONENTS** **29**
- 5.1 Blackbaud CRM Environments Infrastructure 29
- 5.2 Business Processes 30
- 5.3 Online Elements 33
- 5.4 Conversion Approach 35
- 5.5 Data Conversion Functional Areas 35
- 5.6 Data Conversion Assumptions 38
- 5.7 ResearchPoint Conversion 39
- 5.8 Custom Solutions 39
- 5.9 Adoption Readiness & Training Program Components 41
- 5.10 Software Version Scope 45
- 5.11 Language, Currency, Site Security and Location 45

1 EXECUTIVE SUMMARY

This Statement of Work (SOW) outlines the high-level solution, deliverables and estimated costs required to implement an enterprise wide solution for Trinity Health. This Statement of Work (SOW) is subject to the terms and conditions of the Blackbaud Solutions Agreement referenced in the associated Order Form. Throughout this document, Trinity Health will be referred to as "Client" and Blackbaud as "Blackbaud."

1.1 Project Overview

Not-for-profit organizations face a variety of daily challenges, such as building stronger constituent relationships, raising money with increased efficiency, acquiring new donors, retaining donors, and managing effective stewardship. In addition to these challenges, organizations with multiple locations or sites also need a flexible, scalable, and secure CRM solution that addresses their unique needs.

Blackbaud CRM brings together disparate information, such as annual, major, and principal giving, recognition, and analytics, across various sites and programs within an organization. With a single system of record that can be securely and efficiently shared, organizations are able to turn their data into timely, actionable information that maximizes their fundraising efforts, synchronizes campaigns across affiliates, and strengthens relationships with constituents.

1.1.1 Organization Goals

Trinity Health was formed in May 2013 by the consolidation of Catholic Health East and Trinity Health and is one of the largest multi-institutional Catholic health care delivery systems in the nation. When Trinity Health and Catholic Health East closed their consolidation to strengthen their shared mission, increase excellence in care and advance transformative efforts with their unified voice. The consolidated ministry is committed to those who are poor and underserved in its communities and is know for its focus on the country's aging population.

1.1.2 Solution Goals

The overall goal in implementing and utilizing Blackbaud products is to design and implement an effective solution to support specific business needs, to maximize organizational goals, and to achieve user adoption. The primary outcome of implementing this SOW is a working solution that supports the achievement of the organization's critical success criteria, which are stated below.

Key executive requirements in replacing the current systems with the Blackbaud CRM solution are:

- Consolidation of 32 Raiser's Edge databases, one eTapestry database, one DonorQuest database, and one Excel spreadsheet to create one system of record across Trinity Health for enhanced constituent management
- Holisitic, donor-centric view of a constituent and the constituent's relationship to Trinity Health
- Organizational efficiency through improved executive and management level roll-up reporting while eliminating duplication of information technology infrastructure

- Implementation in a manner that maximizes user experience and provides a user-friendly and scalable tool that adapts to the business needs of each end user
- Standardization of processes through a common best practice business model to enable the success of each Regional Health Ministry (RHM) from the largest and most complex foundation(s) to the smaller shops
- Facilitation of professional education and knowledge sharing
- Leverage involvement/influence of governing and foundation boards.
- Production of reports, dashboards, and KPIs to inform and enhance fundraising strategy and build organizational culture to support high performance
- Steamlining day-to-day processes and workflows
- Utilization of best practices for data management and development processes
- Driving alignment between strategic priorities and funding priorities
- Enforcement of business processes and rules

The average duration for implementations from project kick off through stabilization for an implementation approach that includes phased groups of foundations like the one contemplated in this SOW is 12 to 24 months. The specific timeline will be determined as part of this implementation.

1.2 Solution Overview

Trinity Health will implement Blackbaud CRM including Blackbaud Internet Solutions (BBIS). In parallel to the Blackbaud CRM implementation, Trinity Health will implement Financial Edge NXT with a unified Chart of Accounts and TeamRaiser. This SOW covers the Blackbaud CRM implementation with references to the two parallel implementations where dependencies between them exist. The Financial Edge NXT and TeamRaiser implementations are under a separate and unique Statement of Work for each implementation.

In preparation for the implementation, Blackbaud spent several days collaborating with Trinity Health to provide insight into current and future offline and online business processes and conversion requirements.

The Blackbaud CRM implementation will be divided into four implementation groups as described in Section 1.3.

Because Trinity Health is consolidating 35 separate databases into one Blackbaud CRM solution, decisions regarding governance of the database and shared constituent records are critical to user acceptance and adoption of the solution and a successful implementation. The first design cycle in Group 1 is Governance Policy. This cycle will review policy and decisions regarding Trinity Health's governance model.

The use of site for filtering purposes and defined system roles for application users are critical to the adoption of a shared solution. Therefore, system roles will be defined and applied early in the design phase of the implementation. The Security and Administration Design Cycle will precede all other business process design cycles. In lieu of completed system role design, Blackbaud may configure baseline system roles for validation and testing.

To ensure user adoption of business processes, each design cycle after Governance Policy and Security and Administration will include a Client-led teachback session with support from Blackbaud consultants to the RHMs included in Groups 2 through 4 implementations. The teachback sessions will provide the opportunity for Groups 2 through 4 stakeholders to confirm design decisions and provide feedback. Blackbaud also recommends that Trinity Health consider including subject matter experts (SMEs) and other stakeholders from

Groups 2 through 4 as appropriate where expertise may lie outside of the Group 1 SMEs and stakeholders. However, Blackbaud recommends a group of no larger than 15 individuals to participate in a design cycle. These core team members and SMEs will be determining business processes that lay the foundation for a successful Blackbaud CRM implementation and support of Trinity Health's goals and objectives.

Blackbaud will implement custom developed solutions specific to Trinity Health requirements that are identfiied in this SOW. The custom solutions indicated will be presented through functional specifications and wire frame walkthroughs. During the business process design sessions, Blackbaud will gather and review specific requirements for custom solutions in their related functional areas including custom reports.

1.3 Project Approach

Trinity Health has a total of 35 separate source databases across the system that will consolidate into one Blackbaud CRM database which includes 32 instances of The Raiser's Edge, 1 instance of eTapestry, and 1 instance of DonorQuest. One foundation tracks its data in an Excel spreadsheet.

To accomplish this implementation, the project will be divided into four implementation groups. Groups 1 and 2 will consist of nine (9) source database conversions or imports within each group. Groups 3 and 4 will consist of eight (8) source database conversions or imports within each group. Business process design and key decisions related to requirements to fulfill solution goals will take place during Group 1 implementation. Rather than a full conversion, Blackbaud recommends importing data from the eTapestry database and the Excel spreadsheet. A Blackbaud functional consultant will assist Trinity Health with the import of this data.

1.3.1 Group 1 Implementation Overview

Trinity Health Regional Health Ministries (RHMs) selected for Group 1 are a representative sample of all Trinity Health foundations in terms of staff size and dollars raised. Group 1 RHMs have the resources necessary to commit to supporting the early phases of the project. The time commitment for the RHMs participating in Group 1 is significantly greater than the following groups. Group 1 foundations will guide the solution design and define Trinity Health business processes related to Blackbaud CRM, including online solutions. Group 1 participants are responsible for testing and validating business processes as defined during design and conducting teach back design walkthroughs to Groups 2 through 4. Group 1 RHMs will guide decisions regarding the standard data map that will be used for converting data from foundations that are part of future stages.

For Blackbaud Internet Solutions (BBIS) online solutions, the intent of Group 1 is to design and implement a "Trinity Health Standard Internet Configuration" as an initial baseline of core online fundraising and eMarketing functionality that can be deployed to each RHM with a minimum of changes. This SOW assumes that Blackbaud will facilitate the initial configuration of the Trinity Health Standard Configuration for one (1) hospital foundation multi-site, after which Trinity Health staff will deploy the standard configuration to all remaining hospital foundation multi-sites in Group 1 and subsequent group implementations.

Two custom post to general ledger interfaces – one for PeopleSoft and one for Financial Edge NXT – will be developed and tested in Group 1.

Group 1 RHMs include:

1. TBD
2. TBD
3. TBD

4. TBD
5. TBD
6. TBD
7. TBD
8. TBD
9. TBD

1.3.2 Groups 2 through 4 Implementation Overview

The remaining RHMs not included in Group 1 are distributed among Groups 2 through 4. RHMs identified for Groups 2 through 4 will adopt business processes defined in Group 1. These subsequent groups will have their data converted according to the data map defined during Group 1. RHMs will have some minor input for how certain data elements may be mapped for RHM-specific needs. RHMs may also provide minor input for online configurations that are RHM-specific. However, the majority of the data to be converted and web components to be configured will follow the pre-defined model established during Group 1 implementation.

2 PHASES AND DELIVERABLES

Blackbaud follows the Project Management Institute's methodology to implement its solutions. Phases include Initiating, Planning, Executing, Monitoring & Controlling and Closing. Within the Executing phase, activities are further categorized into sub-phases of Design & Build, Test and Deliver & Stabilize.

2.1 Responsibility Matrix

A responsibility assignment matrix, (also known as RACI matrix) describes the Deliverables and each party's respective role related to each Deliverable. Deliverables are those items specifically identified as a "Deliverable" in this SOW. The table below provides an overview of categories of responsibility.

Category	Definition
Responsible (R)	The party who does the work to achieve the Deliverable. One party is assigned as the responsible party, although other parties are delegated to assist as required.
Accountable (A)	The party ultimately answerable for the correct and thorough completion of the Deliverable. An accountable party must sign off (approve) on work that the responsible party provides. One accountable party is assigned for each Deliverable.
Consulted (C)	The party who is consulted before a decision or action is taken. Consulted parties are not expected to produce the Deliverable, but instead provide general advice concerning the Deliverable.
Informed (I)	Those parties who are kept up-to-date on progress, often only on completion of the Deliverable.

2.2 Group 1 Deliverables

Group 1 includes all deliverables related to the full implementation of Blackbaud CRM. With the exception of the Project Plan deliverable, all deliverables listed below refer explicitly to the deliverables of the Blackbaud CRM implementation. The deliverables for the Financial Edge NXT and TeamRaiser implementations are listed in their respective SOWs.

Deliverable	Description	Phase	Client	Blackbaud
Project Charter	The project charter defines project governance, project success factors, and key project resource roles. It formally authorizes the project.	Initiating	A, R	C
Project Plan	The project plan identifies milestones, tasks, durations, resources, and constraints. Note: To ensure an integrated workflow and in consideration of project dependencies, the project plan will be inclusive of the Blackbaud CRM, Financial Edge NXT, and TeamRaiser	Planning	A, C	R

	implementations.			
Project Management Plan	The project management plan outlines key project management practices to be used during the implementation, including: • Status reporting and communications • Change control • Issue management • Risk management • Requirements management	Planning	A, C	R
Implementation Plan	The implementation plan defines how the project will be executed. It includes information for all areas of the project, including • Business Process Design • Conversion • Configuration and Environment management • Custom solutions • Adoption Readiness and Training • Test • Support • Acceptance Criteria	Planning	A, C	R
Grateful Patient Custom Solution User Guide	The user guide outlines the functionality contained within the Grateful Patient Custom Solution as well as the needed use cases and test scripts to effectively test the solution.	Initiating	C	R, A
Adoption Readiness Impact Analysis Findings	Developed through interviews of key project stakeholders and an e-survey of the broad user community, this analysis identifies the organizational impact of the implementation, including: • Relevant business areas and their readiness for change • Risks and the specific mitigation plan for risks	Planning	A, C	R
Adoption Readiness Communications Plan	The results of the Impact Analysis will be used to create an initial communications plan, which will be detailed in concert with the Client's Adoption Team during a	Planning	A, R	C

	workshop. It is the ultimate responsibility of the Adoption Team to execute on the communication plan. The Client will determine which staff is on the Adoption Team with Blackbaud's guidance.			
Adoption Readiness Workshop/Coaching and Intervention	Blackbaud facilitates a leadership workshop to train client staff on the principles of change and how to guide an organization through it, including setting expectations, dealing with resistance, crafting messaging, persuasive techniques, and clarifying uncertainty. Key components of this training are shared with Adoption Team in the communications workshop. Blackbaud will create a plan for monthly office hours for coaching Client Adoption Readiness team members on messaging change to end users. In addition, Blackbaud will identify and address risks related to end-user adoption and devise strategies to mitigate. This could be through additional communication or individual coaching sessions.	Planning	A, C	R
Project Kickoff Presentation	Presentation of the implementation methodology to project stakeholders to build awareness and generate support. Note: This presentation may be combined with elements of the Financial Edge NXT and TeamRaiser implementations.	Planning	A, C	R
Data Dictionary for DonorQuest	A description of all data elements, containing names, structures, and information about usage of non-Blackbaud legacy databases to be converted.	Planning	A, R	I
Source Data	SQL backup files from 32 Raiser's Edge databases. The source data for each database will be delivered within the implementation group to which the RHM is assigned (Groups 1 through 4).	Planning	A, R	I
CSV File	A CSV file for the 1 eTapestry database	Planning	A, R	I

	for import into Blackbaud CRM. The file will be delivered within the implementation group to which the RHM is assigned (Groups 1 through 4)			
Excel Spreadsheet	A copy of the Excel spreadsheet for import into Blackbaud CRM. The file will be delivered within the implementation group to which the RHM is assigned (Groups 1 through 4)	Planning	A, R	I
Entity Relationship Diagram for DonorQuest	An entity relationship diagram that provides an overview of each relational data source. The diagram for the database will be delivered within the implementation group to which the RHM is assigned (Groups 1 through 4).	Planning	A, R	I
Source Data Extract for DonorQuest	Extraction files from source system(s). The source data for the DonorQuest database will be delivered within the implementation group to which the RHM is assigned (Groups 1 through 4).	Planning	A, R	I
Solution Architecture Document	The solution architecture document outlines recommended hardware and software specifications, supporting environments, technical training, and upgrade process.	Planning	A, C	R
Interactive Technical Requirements Document	This form will gather information about SSL, DNS, web server configuration, and other web technical requirements.	Planning	R, A	C
Implementation Environments: • Training • Sandbox • Conversion • Configuration • Design • Development Source Control	Implementation environments required for the implementation will be installed and configured following the guidelines outlined in the solution specific components section of this document. These environments are dependent upon the information outlined in the Blackbaud Hosting agreement.	Planning	A, C	R
Project Collaboration	Project Collaboration Site (SharePoint	Planning	A, R	C

Site	and JIRA) to facilitate collaboration on the project. These sites will contain the following: • Issues List • Configuration List • Action Items List • Project Documents • Project Calendar • Environment List			
Project Management Controls	The following artifacts will be used to monitor, control and communicate project progress. • Status report • Budgetary tracking • Steering Committee presentation • Risk Log • Issue Log • Change Log • Change Order	Monitoring & Controlling	A, C	R
Data Mapping Document	Documents that profile source data, captures data mapping, records translation criteria, and tracks mapping, and progress for each of the 32 Raiser's Edge databases and 1 DonorQuest database. The data map(s) for each will be delivered within the implementation group to which the RHM is assigned (Groups 1 through 4). See Section 2.3 for specific Groups 2-4 data map deliverables.	Executing - Design & Build	A, C	R
Data Conversion Criteria	This list will define the quantitative and qualitative criteria used to confirm the data conversion elements.	Executing - Design & Build	A, R	C
Data Profile Reports	Reports that provide details regarding data hygiene, data format and data counts from Client source system with each data set delivered by Client.	Executing – Design & Build	A	R
Data Conversion Requirements Document	A document that outlines the key data requirements, which will be used to program the conversion.	Executing – Design & Build	A, C	R
Data Conversion Code	Develop, execute, and unit test a conversion program process that uses the	Executing - Design &	A, C	R

	approved Data Conversion Requirements document to migrate source data sets. See Section 5.4 for number of test runs to be performed and delivered.	Build		
Data Conversion Summary Report	A report that provides a summary of converted data, including exceptions.	Executing - Design & Build	I	R
Business Process Design Documents	Each design cycle will have a supporting design document that outlines the key business processes which meet the requirements. The design document will state the key decisions that affect the process, business considerations, required inputs and expected outputs. After the initial delivery, one (1) round of revisions after Client Core Team review, one (1) round of revisions after Client Core Team teach-backs, and one (1) round of revisions after design validation with acceptance of the design document, Client will be responsible for the maintenance and future revisions to the documentation.	Executing - Design & Build	A, C	R
Grateful Patient Solution Configuration Decision Document	A document outlining the Client's final decisions based on the configuration assumptions in the User Guide required for the Grateful Patient solution to work correctly.	Executing – Design & Build	A, C	R
General Ledger Design Guide	A document that details the design, logic, structure, and configuration of the general ledger design and solution between Blackbaud CRM and PeopleSoft and Blackbaud CRM and Financial Edge NXT.	Executing – Design & Build	A, C	R
Fundraising Chart of Accounts	The Chart of Account that lists the full account string for all development office accounts that receive fundraising revenue.	Executing – Design & Build	R	A, C
Configuration Log	A spreadsheet of solutions that have been configured in the system to support business process design decisions. Blackbaud will develop and maintain a record of configuration items that will be	Executing – Design & Build	A, C	R

	used for testing and then for configuring the production system. The configuration log will serve as the document of record for configurations that exist in Client's production system. Client will have full visibility into the log, but will not have the ability to edit the log.			
BBIS Online User Experience Design Document	Outlines goals for the website, prioritizes target audiences and outlines the general phase approach for the implementation. The document will also outline the user experience and page flow for each of the online forms implemented by Blackbaud.	Executing - Design & Build	A, C	R
BBIS Online Cutover Plan	This plan identifies the configuration management plan for launching the website.	Executing – Design & Build	A, C	R
BBIS Email program	Includes tools, templates and business processes to send bulk email. Will include website pages to support opt-outs and communication preferences. See Solution Specific Components for more detail.	Executing – Design & Build	A, C	R
BBIS Website	A configured website based upon the elements outlined in the Solution Specific Components. Trinity Health will determine which hospital foundation site will be the configuration site built out by Blackbaud as a part of implementation.	Executing - Design & Build	A, C	R
Online content migration	Website staff will input all content and any additional pages other than what is outlined in BBIS Solution Specific Components.	Executing - Design & Build	A, R	C
Report/Output Inventory	Client will create, prioritize, and maintain a list of all output needs that are warranted by the design teams, departments, or end users. Outputs can include KPIs, reports, alerts, queries, smart queries, data lists, or exports. Client will develop and maintain a register of all outputs that will need to be configured, tested, and put into	Executing – Design & Build	A, R	I, C

	production. This inventory will be reviewed during each design session to determine the breakout of work effort and responsibilities for developing data outputs between Blackbaud and Client.			
Blackbaud Data Warehouse Refresh Configuration	A configured routine to enable a regular nightly refresh and simple "one click" on demand refresh of data from Blackbaud CRM to the Data Warehouse.	Executing – Design & Build	A, C	R

Custom Solution and Interface Specifications	The following Custom Solutions and Interfaces will be delivered by Blackbaud:
	• Two (2) custom Post-to-GL (PTGL) files
	  o 1 Financial Edge
	  o 1 PeopleSoft
	• Grateful Patient Custom Solution (RCP)
	• Auto File Downloader (RCP)
	See Section 5.8 for solution specific components.
		Executing - Design & Build	A, C	R

Post Go Live Support Environments • Testing • Training • Staging • Development	The staging environment will be deployed as an ongoing final testing environment prior to Production; the Staging and Production environments should be logically configured as similarly as possible. The Test, Training, and Development environments will remain in use post go live for training and system enhancement activities.	Executing - Design & Build	A, C	R
Test scenarios	Test scenarios will be created by the Client team during the design cycles for design and website validation. Additional test scenarios will be created by the Client team based on the use cases provided in the Patient Guide for the Grateful Patient Solution. Any test scenarios or use cases required beyond those in the Patient Guide are the responsibility of the Client. While Blackbaud may provide guidance	Executing - Design & Build	A, R	C

	as needed, Client is solely responsible for the creation and maintenance of use cases or test scenarios and all related test script and use case documentation.			
User Acceptance Test Scripts	Detailed test scripts will be created by the Client team during Design phase for use by the Client team during integrated user acceptance testing. Blackbaud will provide test script templates and guidance in developing test scripts for validation of business process design, conversion, and custom solutions. Client is responsible for creating the business use cases and accompanying test scripts.	Executing - Design & Build	A, R	C
Standard Training Workbooks	Printable PDF guides that accompany instructor-led training during the Project Team Training phase. One copy per participant (up to 20) included in each delivery, prior to Project Team Training session.	Executing – Design & Build	A, I	R
Training Needs Analysis	This two-page document provides an overview of findings from the Training Needs Analysis Workshop, including current strengths and weaknesses, opportunities and threats/risks for future training.	Executing – Design & Build	A, C	R
Training Plan	A training plan is the deliverable created from a training needs analysis. It documents the training strategy that is recommended for your organization based on the results of the analysis.	Executing – Design & Build	A, C	R
User Acceptance Tests	Conduct tests using data that was converted in Test Runs. Tests should assess both data conversion and end-to-end business processes. Tests for both Blackbaud CRM and Blackbaud Internet Solutions features, which can occur independently except for the business processes that directly relate to the data that is passed from online to offline. The interconnected business processes will need to be tested at the time of the implementation of Blackbaud	Executing - Test	A, R	C

	Internet Solutions.			
User Acceptance Testing (UAT) Issue Log	An issue log will be maintained during UAT to confirm test scripts have been completed, issues identified and end-to-end testing has occurred. This log will be created and maintained by Client and housed on the project collaboration site (JIRA or SharePoint). Any issue needing resolution by the Blackbaud team must exist on the UAT issue log.	Executing – Test	A, R	C
Cutover Plan	A cutover plan will outline the priorities, tasks, and procedures during the cutover period. It will also include the contingency plan for potential risks.	Executing – Test	A, C	R
Environments • Production	The production environment will include the final conversion run, configurations, custom solutions, custom reports, and interfaces. Only approved configurations that exist in the configuration log and any related design documents will be included in production environment.	Executing – Test	A, C	R
Adoption Readiness Assessment report	A report based on an e-survey of the user community to assess project communications effectiveness, project involvement, and readiness for implementation	Executing – Test	A, C	R
Updated Communications Plan	Post-live adoption workshop(s) provide feedback to update the communications plan	Executing – Test	A, C	R
Jumpstart Delivery Content	In addition to standard workbooks that will be delivered as a part of the training, Client will receive workbooks in an editable format in order for the Client to edit and tailor the workbooks for specific information.	Executing – Deliver & Stabilize	A, C	R
Policy and Procedures Guide	End-user documentation outlining important system codes and standards for use. The information used to create the guides will be based on the design documents. All policy and procedure guides will be created and maintained by Client.	Executing – Deliver & Stabilize	A, R	C
End User Training	A Trinity Health trainer will train the Group 1 end-user community on functionality of	Executing – Deliver &	A, R	C

	Blackbaud CRM within the context of the organization's business design. Trinity Health will be responsible for preparing the JumpStart Delivery content for end user training.	Stabilize		
Source code	All source code created during this implementation for customizations, custom reports, and integrations will be provided to Client and to Blackbaud Support.	Executing – Deliver & Stabilize	A	R
Final Data Conversion (Production) database	The final data conversion includes a delivery of a Blackbaud CRM database containing all approved requirements.	Executing – Deliver & Stabilize	A	R
User Adoption e-survey	Post go-live, an e-survey will be used to assess the degree of user adoption and utilization of the solution's functionality.	Closing	R	C

2.3 Groups 2 through 4 Deliverables

Groups 2 through 4 implementation includes deliverables related to the execution phase of the implementation for the RHMs within the groups.

Deliverable	Description	Phase	Client	Blackbaud
Updated Data Mapping Document	Provide a database-specific data map for each database to be converted based upon the agreed upon map in Group 1 and accounting for agreed upon RHM-specific needs. The data map for each database will be delivered within the implementation group to which the RHM is assigned (Groups 2 through 4).	Executing – Design & Build	A, C	R
Refined Business Processes	Provide up to three (3) specific business processes per RHM that are required above and beyond agreed upon business processes as defined in Group 1. Processes will be delivered for each group implementation.	Executing – Design & Build	A, C	R
Data Conversion Criteria	This list will define the quantitative and qualitative criteria used to confirm the data conversion elements.	Executing - Design & Build	A, R	C

	Criteria will be delivered for each group implementation.			
BBIS Online Configuration Surveys	Each RHM will complete a brief survey created by the Client regarding online options. Trinity Health's web team will configure each RHMs web forms based on the responses to the survey.	Executing - Design & Build	A, R	C
Cutover Plan	A cutover plan will outline the priorities, tasks, and procedures during the cutover period. It will also include the contingency plan for potential risks. A cutover plan will be delivered for each group implementation.	Executing – Test	A, C	R
Data Conversion Code	Develop, execute, and unit test a conversion program process that uses the approved Data Conversion Requirements document to migrate source data sets. See Section 5.4 for number of test runs to be performed and delivered.	Executing - Test	A, C	R
BBIS Internet Solutions Configuration	Trinity Health's web team will configure web forms within Trinity Health's Standard Internet Configuration specifically for each RHM, based on responses to the Web Planning Surveys. Configuration will be delivered for each group implementation.	Executing - Test	A, R	C
Leader Training on Supporting Change and Dealing with Resistance	Hold a training session for 10-12 attendees, jointly determined by the Client and Blackbaud, to prepare attendees to deal with resistance and help with the transition to go live. A training session will be delivered for each group implementation.	Executing - Test	A, C	R
End User Training	A Trinity Health trainer will train the end-user community on functionality of Blackbaud CRM within the context of the organization's business design. Trinity Health will be responsible for preparing the JumpStart editable content for end user training. End user training will be delivered for	Executing – Deliver & Stabilize	A, R	C

	each group implementation.			
Final Data Conversion (Production) database	The final data conversion includes a delivery of a Blackbaud CRM database containing all approved requirements. The final data conversion for each database will be delivered within the implementation group to which the RHM is assigned (Groups 2 through 4).	Executing – Deliver & Stabilize	A	R
Project closure report	The Project Closure Report is the final document produced for the project and is used by senior management to assess the success of the project, identify best practices for future projects, resolve all open issues, conduct lessons learned and formally close the project. The report from the user adoption e-survey is included in the Project Closure Report The Project Closure Report will be delivered upon completion of all four implementation groups.	Closing	A, C	R

3 ASSUMPTIONS & CLIENT RESPONSIBILITIES

The performance of Services, timing, resources and fees associated with this SOW are based on the assumptions and Client responsibilities set forth below. Should any of these assumptions not be fully realized or should Client fail to timely perform its responsibilities below and elsewhere in this SOW, a Change Order shall be required resulting in adjustment of the fees, expenses, and schedule associated with this SOW.

3.1 General Assumptions & Responsibilities

- Client shall provide resources to fill the following core roles:
    1. Project Manager, who will work with the Blackbaud Project Manager to co-ordinate meeting resources, assist with Project planning, help resolve issues / manage risk, provide feedback for initiative prioritization, assist with roadmap production and ensure that appropriate management approvals are obtained in a timely manner.
    2. Business and Technical Subject Matter Experts as needed to attend various sessions. They will provide knowledge and insight into the data, processes and tools for each activity being investigated. Additionally, Client resources will be available to provide follow up materials and answer questions after sessions have concluded, and provide feedback on associated Deliverables.
- Client shall provide Blackbaud with timely and complete access to, and ensure the availability of, all Client personnel, data, documentation, information, standards, systems and other resources that may be reasonably necessary for Blackbaud to perform the Services.
- Client acknowledges and agrees to provide Blackbaud with prompt and adequate responses to its requests for information and other requests related to the Services to be performed under this SOW. In the event that Blackbaud has made a request and Client has not responded promptly with the requested information, Blackbaud may issue a "Final 30-Day Project Notice" ("Final Notice") to Client. If Client does not respond as requested to the Final Notice, Client agrees that Blackbaud shall be relieved of any further obligations which have not been completed under the SOW and Client shall remain liable for payment of all Services fees as set forth herein. Any and all services requested by Client following the expiration of the aforementioned thirty (30) day period will require Client and Blackbaud to execute a new SOW and Client shall be responsible for any additional Services fees contemplated there under, even if listed in the original SOW.
- Client will cooperate with Blackbaud in taking actions and executing documents, as appropriate, to achieve the objectives of this SOW. Client agrees that Blackbaud's performance is dependent on Client's timely and effective cooperation with Blackbaud. Accordingly, Client acknowledges that any delay by Client may result in Blackbaud being released from an obligation or scheduled deadline or in Client having to pay additional fees for Blackbaud's agreement to meet a specific obligation or deadline despite the delay.
- Client is responsible for the completeness and correctness of all documentation presented to Blackbaud, and shall verify the accuracy and completeness of the information provided.
- Client shall ensure the cleanliness of all data presented to Blackbaud and shall verify the accuracy and the cleanliness of the data. Data shall be transferred from the source system to the Blackbaud system. While Blackbaud may provide limited support for data testing as specified in the Deliverables section, Client remains responsiblo for data testing, data cleanup, data setup, the resolution of source data defects (both during the Project and Post-Implementation stabilization period).

- Blackbaud is not responsible for client data clean-up, and no effort will by made by Blackbaud to clean up client data through the conversion or any other aspect of the implementation.
- Client shall be responsible for providing a reliable method for matching associated data otherwise, it will not be linked during the data conversion.
- Client is responsible to provide sufficient facilities, workspace, printers, desktop hardware and software, network access, email, system access, and building access for the project team resources.
- Client shall ensure resources complete any foundational training required prior to taking a Blackbaud training course.
- Client is responsible for working with applicable vendor(s) for the resolution of defects in all third-party software and to resolve defects in Client's legacy applications.
- Client's business leaders will be responsible for timely decision making, critical issue resolution, and efforts to promote this Project internally as defined by project governance.
- Client will notify the appropriate vendors and make the necessary arrangements for Blackbaud to conduct interviews to gather details about the vendor's processes.
- Blackbaud is not responsible for any modification or other change made to any Deliverable by Client or a third party.
- Completion of Deliverables assumes Client resources (e.g., business leaders, team members, IT resources, business Subject Matter Experts (SME), etc.) are available to support activities such as workshops, meetings, document review sessions, etc. If Business SMEs cannot provide adequate time, the Deliverable schedule and activities are subject to change.
- Client will provide the necessary business/IT experts and decision makers to attend and support the work sessions. Blackbaud will assist Client with the identification of the necessary participants.
- Interfaces shall be contained in delimited flat-file format, unless otherwise mutually agreed upon, and dropped in network locations accessible from the production Blackbaud CRM environment. This does not preclude the use of other formats including real-time interfaces, but such changes may result in increased effort.
- Blackbaud adheres to the policies outlined by the PCI Security Standards Council to prevent the retention of sensitive data beyond business requirements. For test conversions performed by Blackbaud Professional Services, the full Primary Account Number (PAN) shall not be converted for constituent records; the test conversion will be limited to the last four digits. However, the full PAN shall be converted to the credit card number field during the final conversion.
- Client shall identify an approved credit card payment processor that is compatible with one of the approved Blackbaud Payment Services (BBPS) gateways, located at www.blackbaud.com/bbms/bbms-tier3.aspx.
- Client acknowledges and agrees that there are potential issues and risks in situations in which they copy production data containing login credentials for any "Cloud Service" into non-production environments. This includes, but is not limited to, Blackbaud Payment Service, Blackbaud Merchant Services, and Email Services. Specifically, Client understands and acknowledges that the following issues and risks arise if client does not create merchant accounts for testing purposes:
  - If the merchant account is used in "live" mode, "test" transaction(s) will be processed as if it is a real transaction; i.e. if the credit card number is real, the credit card will be processed and charged for the amount of the test transaction.

- If Client puts their production Blackbaud Payment Services merchant account in "demo" mode to process the "test" transaction, subsequent "real" transactions in the production environment will not be processed, even though the eCRM application will receive a return authorization code.
- Additionally, Client understands and acknowledges that the following issue and risk may arise for any email processed within a non-production environment: Any email processed through the system using "production" credentials will be treated as live email and will be sent to all selected recipients. Blackbaud recommends that the client create specific test recipients for any email processed within a non-production environment.

- Client will submit files in one of the following media formats. If data cannot be supplied in one of the following formats, Client and Blackbaud will discuss options.
  - CD or DVD-R
  - Encrypted hard drive
  - Secure FTP (File Transfer Protocol)

3.2 SOW Specific Assumptions & Responsibilities

3.2.1 Data Conversion

A successful data conversion is dependent on the completion of tasks and meeting of deadlines identified in the conversion timeline. It will be the responsibility of both Blackbaud and Client team members to be aware of this timeline and take the appropriate steps to meet the delivery schedule. If tasks are incomplete or deadlines are missed, the project could be delayed.

Blackbaud assumes that Client will have prepared its data across all databases towards a common model goal to reduce the number of data translations required to convert legacy data into one consolidated database with shared business processes and has estimated the number of conversion hours based on this assumption. If data cleanup and preparation is not completed, a Change Order will be required to allow for a larger number of data translations from each legacy database map. To assist Client in this preparation, Blackbaud can provide a script that shows table entries per category so Client can identify differences across the databases and address appropriately before conversion.

Blackbaud assumes that current business processes adhere to standard use of the Raiser's Edge and/or DonorQuest database functionality (i.e. Events track event information, Memberships track membership information) and that Client has not introduced workaround solutions for business processes that use non-standard functionality. If data elements are being used for a workaround solution in a non-standard format than the way the product was designed to function, a Change Order will be required to address additional data mapping and translations required to meet designed business processes in Blackbaud CRM.

3.2.1.1 Data Cleanup

The focus of the data conversion process is to convert the data from the legacy database systems as they currently exist into the Blackbaud database system. The conversion process, therefore, is not intended to assist in cleaning up or correcting erroneous data elements in the legacy data systems.

All customers need to conduct some data cleanup, to some degree. Data integrity problems encountered will be identified throughout the implementation and testing of the conversion. Blackbaud assumes that Client will investigate options such as pre-conversion and post-conversion data cleanup to address these issues.

3.2.1.2 Pre-Conversion Data Cleanup

The Client conversion team is encouraged to develop a plan and execute targeted data cleanup before the final conversion, or during the test runs as source data issues become apparent. However, once the initial data extraction has been conducted, the legacy data records or table structure should not be modified without first consulting with the Blackbaud conversion analyst, as such changes may have impact on existing logic.

Pre-conversion data cleanup changes should generally be made to the actual data within the legacy system; otherwise, Client assumes greater risk that changes made to the extracted database table or record structure will require additional mapping, data extractions, work effort, time, and financial investment to complete the project.

3.2.1.3 Post-Conversion Data Cleanup

It is quite normal to have a variety of post-conversion data cleanup tasks to perform after a final conversion. The Blackbaud consultant and conversion analyst will assist in identifying post-conversion cleanup tasks and suggest recommended resolutions when possible. Post-conversion cleanup tasks will be executed by the Client team, with the support of the Blackbaud implementation team.

3.2.1.4 Final Run Conversion to Production for Groups 2-4

Because each Group will have its own go live date, there will be downtime in the production database as Groups 2-4 go live. The downtime allows for uploading of the final conversion run and validation. The specific amount of downtime will be determined by the Blackbaud and Client project managers based on the conversion requirements.

3.2.2 ResearchPoint Conversion

Conversion of any ResearchPoint database is not included in this SOW. If conversion is desired, a Change Order will be required to complete the conversion.

ResearchPoint and WealthPoint data that already exists in the Raiser's Edge databases will be converted. RHMs that have imported ResearchPoint and WealthPoint data into existing Raiser's Edge databases must ensure data is up to date for accuracy of the conversion data.

3.2.3 Post to General Ledger Processes

The Post to General Ledger processes identified in this SOW assume that Client will have a unified Chart of Accounts that each RHM uses as its standard. As per the Client and with Blackbaud's agreement, General Ledger Integration Design must be one of the first decisions made by Client's Philanthropy Program Steering Team. Trinity Health will have one Philanthropy Chart of Accounts whereby each RHM Foundation Chart of Account data will roll up into.

3.2.4 Grateful Patient Custom Solution

The Grateful Patient Solution assumes the following:

- This SOW will include conversion of grateful patient data from the legacy system to Blackbaud CRM if supporting data exists in the legacy database.
- If Client requires existing constituent records to be updated with the Grateful Patient solution, a Change Order will be necessary to account for the export of existing data based on specific Client criteria from Blackbaud CRM for import back into the system.
- Specific configuration assumptions are made for the Grateful Patient solution to function as designed. Client is responsible for making decisions related to the required assumptions.
- Client is responsible for any manual preparation of the patient data file required due to the output fields from the patient data system extract for import in to Blackbaud CRM.
- The solution does not include custom import of prospect ratings and/or screening data from third-party screening applications.

3.2.5 Blackbaud Internet Solutions

The Blackbaud Internet Solution Implementation approach assumes the following:

- The Client will reproduce the final visual design of the defined RHM websites within Blackbaud Internet Solutions during the duration of this project, including the necessary Stylesheets, Layouts, Templates and Javascript to replicate the design.
- Client is responsible for migration of all content and pages from Blackbaud NetCommunity to Blackbaud Internet Solutiens.
- Client is responsible for the creation of each RHM's Blackbaud Internet Solutions multi-site based on the framework provided by Blackbaud.
- Blackbaud will deliver a one (1) day overview of Blackbaud Internet Solutions during the Core principles design cycle to support design conversations.
- The COER – Customized Online Event Registration form will not be implemented within Blackbaud Internet Solutions. A change order would be required to include this feature into the product.
- The Advanced Donation form will not be developed or implemented by Blackbaud. Training will be provided to teach the client how to develop and configure the form but it will be the responsibility of the client to self implement the functionality.
- The Client will receive access to the Blackbaud Internet Solutions configuration environment at the conclusion of validation of Blackbaud Internet Solutions forms and sign off on the completion of work by Blackbaud.
- RHMs who currently use Constant Contact or other email solutions will use Blackbaud Internet Solutions upon implementation.

3.2.6 TeamRaiser Peer-to-Peer Fundraising Implementation

TeamRaiser will replace any peer-to-peer fundraising solution that RHM's may currently use. The TeamRaiser implementation for RHM Foundations that have this functionality today is under a separate and unique Statement of Work. Other RHMs that want to start a peer-to-peer fundraising program will use TeamRaiser and will be trained on the set up and use of the solution after the Groups 1-4 implementation of Blackbaud CRM is complete.

This SOW and the TeamRaiser SOW will be implemented simultaneously. The Engagement Manager for the project will oversee the implementations and any dependencies through an integrated project plan.

3.2.7 Training

The Training Program assumes the following:

- Client is responsible for End User Training and associated training materials using Jumpstart Delivery Content. If Client resources are not available for delivery of end user training or if Client determines that Blackbaud will lead end user training, a Change Order will be necessary to make available Blackbaud trainers to supplement Client resources.
- If the Training Needs Analysis determines a need for a formal learning assessment after end user training, Client is responsible for the development of the assessment tool(s). If Client requires Blackbaud development or support of the development of the assessment tool, a Change Order will be necessary.

3.2.8 Reporting

Blackbaud and Client will work together to identify critical reports and determine the appropriate output including KPIs, standard reports, alerts, queries, smart queries, data lists, or exports. If no out-of-the-box outputs meet Client's needs and a custom report is required, Blackbaud and Client will gather requirements for the report and determine work effort. Client is responsible for developing the custom report with mentoring support and guidance from Blackbaud.

3.2.9 Mergers and Acquisitions of Additional Foundations

The current SOW includes the conversion of 32 Raiser's Edge databases and one (1) DonorQuest database. Additionally, the one (1) eTapestry database and the one (1) Exel spreadsheet will be imported or re-keyed as determined by the Blackbaud and Client project managers. If additional foundations are acquired during the project implementation and Client intends to include them in the database consolidation, a Change Order will be required for the additional conversion and project deliverables. For specific requirements, please reference the MSA.

3.2.10 Financial Edge NXT Implementation

Financial Edge NXT will be used by RHMs for foundation accounting purposes. Client's future cost accounting system must integrate with Financial Edge NXT. The Financial Edge NXT implementation and integration is under a separate and unique Statement of Work and Order Form.

3.2.11 Target Analytics

Blackbaud and Client will initiate new wealth screening processes after Blackbaud CRM is live and all RHM data is converted. The Target Analytics implementation is under a separate and unique Statement of Work and Order Form.

4 FEES, BILLING AND CHANGE ORDERS

4.1 Estimated Services

The services listed below represent an estimate for the implementation of Blackbaud CRM.

Service Description	Quantity	Rate	Fee	Billing Code	Billing Terms
Implementation Services	9037	$200	$1,807,400	IMBBCRMTM	T&M
Implementation Services	2500	$200	$500,000	IMBBCRMTM	T&M-100%
Services Delivery Total			$2,307,400		

4.2 Billing Terms

Billing Terms	Description
T&M	The professional services described here are provided on a time-and-materials (T&M) basis only. The estimate(s) cited above represents an estimate only and does not reflect any binding obligation for Blackbaud to complete those services within the estimated time or cost. Any required changes to the estimates will be processed with approval as defined in the Change Order section of this agreement. Upon signing and returning the Order Form, Blackbaud shall invoice for services rendered based on the number of hours expended by Blackbaud. These fees do not include any travel-related expenses.
T&M-100%	Upon signing and returning the Order Form, Blackbaud shall invoice for an initial prepayment for implementation services equaling 2,500 hours.

4.3 Implementation Pre-Payment

Client will be invoiced for an initial payment equaling 2,500 hours prior to Blackbaud's delivery of professional services within this SOW. Services and/or activities performed and any deliverables applied to this pre-payment must be those associated with capital budget expenditures to include: project management, technical consulting, custom development, and business intelligence and report development. These 2,500 hours will be billed and credited on a T&M basis until fully expended.

All other professional services delivered, exclusive of training, will be billed as performed and delivered on a T&M basis.

4.4 Change Orders

Blackbaud shall perform the services specified in this SOW. Any other services or changes identified by the parties will require a duly executed Change Order. If the parties mutually agree to change this SOW, then, Blackbaud will create a Change Order documenting the change in Statement of Work, additional (or exchanged) services to be delivered and resources required, any changes to the project plan and/or deliverable dates (if applicable), and additional estimated fees (if applicable).

Both parties must properly execute the change order before any resources will be assigned or any additional/changed services will be performed. Any properly executed Change Order is subject to the terms of the Master Software and Services Agreement and this SOW.

4.5 Expiration of Services

If, (i) within one year of execution of the SOW, the Client has not scheduled any work to be performed, or (ii) if the Client has scheduled work to be performed, but due to the unavailability of the Client such work has not commenced within six (6) months of being scheduled, the SOW will be deemed to be terminated by the Client and any fees paid in connection with this SOW shall be retained by Blackbaud and applied toward a cancellation fee.

Prepaid services not scheduled within 18 months shall be deemed expired and any fees paid in connection with this service shall be retained by Blackbaud.

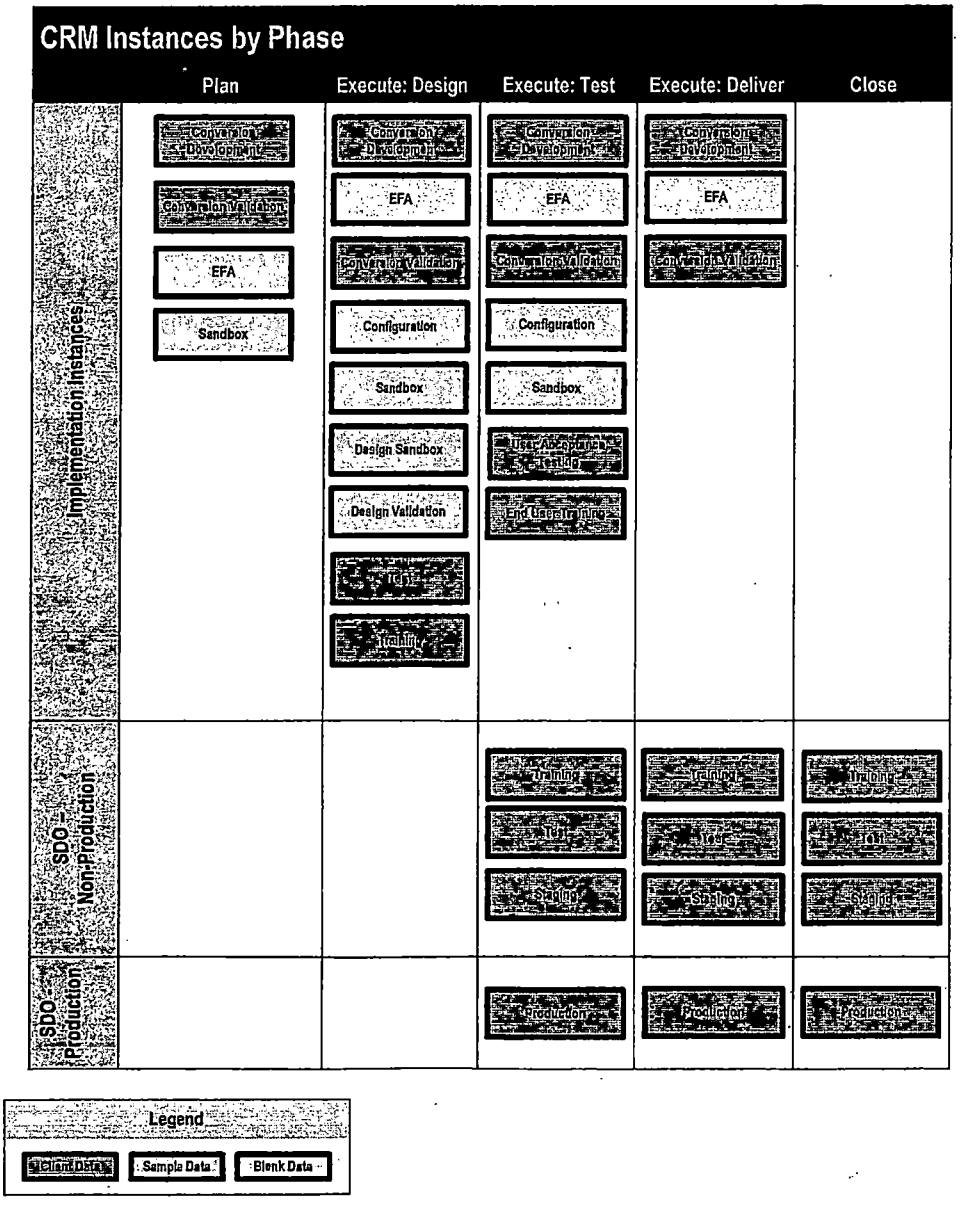
4.6 Cancellation Policy

In the event services are scheduled pursuant to this SOW and the Client cancels or postpones with less than ten (10) business days' notice, the Client shall pay for the committed hours at the applicable rates plus any out of pocket expenses incurred.

5 SOLUTION SPECIFIC COMPONENTS

5.1 Blackbaud CRM Environments Infrastructure

The hardware to support the Blackbaud CRM environments is paid for by the client and provided and maintained by Blackbaud. The following diagram shows the Blackbaud CRM instances required during each phase of the Blackbaud CRM implementation and lifetime.



5.1.1 Implementation Environments

The Implementation environments will exist during the professional services engagement. All implementation environments will be retired after CRM Go-live.

[redacted]	OS –	Windows 2012R2
	SQL Server –	SQL Server 2012
	Disk -	Data - 2500 GB
		Backups – 1500 GB
[redacted]	OS –	Windows 2012R2
	SQL Server –	SQL Server 2012
	Disk -	Data – 1500 GB
		Backups – 700 GB
[redacted]	OS –	Windows 2012R
	Disk -	Apps – 60 GB

5.1.2 Hosted Environment Infrastructure

Blackbaud Hosting will provide 3 non-production environments, Test, Train, and Stage, as well as the Production environment. The total storage allocated to Trinity Health is 9 TB. The hardware resources to support the environments listed will be installed on shared physical and virtual servers. The hosting infrastructure is described in the Hosting and Services Level Exhibit in the Master Services Agreement.

5.2 Business Processes

This SOW is limited to the following business processes. If a business process and supporting information is not explicitly stated below, it is considered out of scope for this SOW and may require a change order if deemed a critical requirement.

Design Cycles	Supporting Business Processes
Governance Policy	Governance policy and decisions will be discussed in this cycle. The following topics are included: • Governance model • Managing shared constituent records • Managing global functionality with impact across all RHMs • Central and local system administrator access • Pre- and post-conversion data cleanup activities identified
Security and Administration	During this cycle, the team will define system roles, task and feature permissions and administrative tasks. The following topics are included: • Security review • Security design and procedures, including governance for shared constituents and shared data elements • Security system roles and permissions

Design Cycles	Supporting Business Processes
	• User profiles • Duplicate record management • Queue scheduling and oversight • Centrally managed database administration and governance • Locally managed database administration and governance • Internal support structure and escalation procedures
Core Principles	Constituent-level business processes and system-wide structure will be explored in this cycle. Core principles include the fundamentals of the CRM and web solution which will affect subsequent design cycles. The following topics are included: • Campaign fundraising structure • Appeal structure • Designation structure • Constituent record management • Membership structure • Revenue and recognition structure • Organizational structure and system access • Online constituent management • Online system Overview of Blackbaud Internet Solutions comparison to Blackbaud NetCommunity • Transaction Processing of Online data • Web Strategy Planning • Related security permissions
General Ledger Account Structure and Integration with Financial Edge NXT and PeopleSoft	This design cycle will focus on General Ledger design. Representatives from Client's finance team should attend this session. The following topics are included: • Designation structure • GL account string structure and design • Transaction and segment mapping • Understanding of the fundraising Chart of Accounts
Revenue Operations and Donor Services	Business processes supporting revenue operations (online and offline) will be examined in this design cycle. The following topics are included: • Revenue processing and workflow • General Ledger interface • Donor acknowledgement and fulfillment • Internet revenue and online giving • Related security permissions • Reporting and output requirements During this design session, peer-to-peer fundraising may be discussed in consideration of the TeamRaiser components that must by synced through the integration solution to Blackbaud CRM.
Marketing & Communications	This design cycle will review all business processes and reporting related to acquiring and soliciting annual fund donors through multi-

Design Cycles	Supporting Business Processes
	channeled direct marketing, communications, and solicitation efforts. The following topics are included: • Marketing strategy and planning • Marketing efforts structure • Appeal mailings structure • Acquisition • Donor retention • Email communication • Inbound requests • General communications • Related security permissions • Reporting and output requirements
Prospect Management Including: • Annual Giving • Major Giving • Planned Giving • Prospect Research • Grateful Patient • Corporate & Foundation Giving	This design cycle will examine the strategies and tactics that drive individual prospect management, prospect research, planned giving, and corporate/foundation giving. The following topics are included: • Prospect research • Prospect assignment • Prospect solicitation lifecycle/moves management steps • Personalized donor acknowledgement • Planned gift vehicle useage • Legacy society considerations • Planned Gift communications • Grants and proposal management • Related reports and data outputs • Related security considerations Additionally, the design elements of the Grateful Patient Solution will be included as part of the overall Prospect Management design cycle.
Stewardship, Recognition & Membership	This design cycle will address stewardship plans and activities, endowment fund stewardship, recognition programs, and giving level programs as well as membership activities related to acquisition, renewal, fulfillment, solicitation, and communication.The following topics are included: • Stewardship plans • Recognition programs • Recognition events • Membership programs • Membership levels and benefits • Contribution-based and dues-based memberships • Membership renewals, cancellations, and transfers • Related security permissions • Reporting and output requirements The membership design cycle defines the business process workflows that enable the effective management of membership programs and members. Key fundraising and member activities occur through the

Design Cycles	Supporting Business Processes
	program, and it is important to effectively track and manage acquisition, renewal, fulfillment, and additional solicitation processes when communicating with members.
Event & Volunteer Management	The business processes that support event management and volunteer management will be explored in this cycle. This includes event budgeting, registration (online and offline), invitation processes, registration fees, and related event solicitation and follow-up activities as well as volunteer application workflow and tasks, job assignments, timesheets, and recognition. The following topics are included: • Event setup • Event registration • Event communication • Application process and screening • Volunteer job assignments • Volunteer recognition • Related security permissions • Reporting and output requirements During this design session, peer-to-peer fundraising will be discussed in consideration of the TeamRaiser components that must by synced through the integration solution to Blackbaud CRM.

5.3 Blackbaud Internet Solutions Online Elements

This SOW is limited to the following online components of BBIS. If a component and supporting information is not explicitly stated below, it is considered out of scope for this SOW and may require a change order if deemed a critical requirement.

5.3.1 Website

Online Element	Supporting Components

Online Design Reproduction	Blackbaud will reproduce the final visual design of the client websites within Blackbaud Internet Solutions (BBIS) once during the duration of this project. Blackbaud will build:
	• Responsive layouts
	  o Overall site layout/wireframe
	  o Up to four mobile responsive layouts will be delivered with up to three mobile breakpoints each (two for the Online Giving site, two for the Online Community site)
	The number included will be dependent on the number of layouts needed to replicate Client (Group 1 Hospital Foundation Multi-site) visual design.

Online Element	Supporting Components
	Responsive layouts accommodate small, medium, and large screen sizes. Typical screen sizes are: • Small (Smart Phones:) Browser windows 0 - 640 pixels wide • Medium (Tablets:) Browser windows 641 - 1023 pixels wide • Large (Desktop and Laptop Computers:) Browser windows 1024 pixels and up • These screen sizes are subject to alteration based on discovery, and if additional sizes are requested, a Change Order may be requested. • Templates o Design of site sections o Up to six templates will be delivered • Cascading Stylesheet o Set up for overall font type, size and color, table format, color schemes, etc. ***Please Note:*** *Unless otherwise stated, there may be elements on Client's existing website that will not be replicated in* ***Blackbaud Internet Solutions****. These include Flash, JavaScript, JavaScript-driven menus, menu animation, search boxes, or other interactive elements that are not inherent in* ***Blackbaud Internet Solutions*** *functionality.*
Online Giving	Blackbaud will build: • Up to five donation forms with batch processing to CRM , using the following as a base: o Standard donation form • Designation search (add only if designated giving is required for more than 10 funds) • Payment page • Five to ten focused content areas • Payment confirmation page • Tell-A-Friend through social integration with up to two social networks (Facebook and Twitter standard; other networks may be additional) • Acknowledgement page and email optimization ***Please Note:*** *The Advanced Donation form will not be developed or implemented by Blackbaud. Training will be provided to teach the client how to develop and configure the form but it will be the responsibility of the client to self implement the functionality.*
Online Events	Blackbaud will build: • Up to three standard event registration form samples • Acknowledgement page and email optimization • Tell-A-Friend though social integration with up to two social networks (Facebook and Twitter standard; other networks may

Online Element	Supporting Components
	be additional) • Optional standalone event calendar with categories
Online Community Microsite	This solution will focus on the top three audiences and includes: • Audience analysis • One user login functionality • Login acknowledgmeent email • One user registration functionality with batch processing into CRM • One return user landing page • Up to twenty content areas, including targeted content • Directory listing • Up to three profile update forms

5.3.2 Email

Online Element	Supporting Components
Email	• Up to three email opt-in forms • Up to three communication preference /opt-out forms • Tell-A-Friend through social integration with up to two social networks (Facebook and Twitter standard; other networks may be additional) • One email newsletter template • Privacy policy page (required to send email)

5.4 Conversion Approach

The conversion will include four (4) full runs – one (1) initial run using the standard Raiser's Edge to Blackbaud CRM data map and initial DonorQuest data map, two (2) test runs, and a Final Conversion.

5.5 Data Conversion Functional Areas

The following table shows the functional areas within Blackbaud CRM. Unless explicitly stated below, any other functional areas are considered out of scope.

Functional Area	Description
Constituents	An entity tracked within the database that can be classified as different types (i.e., individual, organization).
Groups & Households	A type of Constituent that brings multiple constituents together into one record for tracking and recognition. A Household is used for a family, while a Group would be for multiple constituents that are not related.
Relationships	A connection between constituents tracked within the database (i.e. father and son; employee and employer).
Addresses	Physical location where mail can be delivered to a constituent. This could be their Home, Business, Vacation Home or more. Designated by their "type" and tracked on what dates mail can be sent to. If more than one is stored, then one address must be marked as Primary.

Functional Area	Description
Phones & Email	Number or email address that is used to contact a Constituent. If more than one of each type is stored, then one phone number and one address must be marked as Primary.
Notes	Field that contains documentation about various types of records.
Attributes	Client-defined fields created to track additional information about a record that the program does not track by default.
Name Formats	Client defined constituent addressees and saluations. All name formats will convert as free text, without formulas.
Organization Positions	Client-defined organizational hierarchy of staff positions/roles, position holders (staff), and dates of tenure. Used in major giving prospect management and reporting.
Committees	A type of Constituent. Similar to a Group – but can raise money, coordinate an event or have its own goals to specifically help the CRM owner.
Interests	Personal information about a constituent that details items that they are inclined to like or do (i.e. Golf, Volunteer, Library).
Mail Preferences and Solicit Codes	The ability to manage the communication preferences for a constituent to ensure the Client communicates with the constituents in ways they prefer.
Education	A way to keep track of a constituent's education history.
Appeals	A record that tracks a solicitation to your constituents.
Constituent Appeals/Responses	A record that tracks which constituents received certain appeals. Responses are made in reference to these constituent appeals.
Campaign	A planned effort to raise money.
Memberships	A record that allows a Client to create membership programs and tack the constituents who belong to the programs.
Revenue	Records of financial transactions received by the Client.
Matching Gifts	A gift from a company that was made in response to an individual's gift, when that individual has a relationship with the company (typically employee). Pledges will be matched to payments if unique identifiers are provided that link the pledges to the payments. If identifiers are unavailable or unreliable, Client will need to provide a reliable method for matching payments to pledges, otherwise they will not be linked in the conversion. The same process will be performed for installment pledges, soft credits and matching gifts.
Cash Gifts	A gift made with cash. Will often be referred to if a check was used. The program allows you to differentiate between payments by cash and payments by check.
Interactions	Tracking one on one contact (phone, mail, etc.) between the nonprofit and a constituent.
Pledges	A promise to donate in the future. Normally on a set schedule.
Pledge Payments	A payment towards the balance of a Pledge. Pledges will be matched to payments if unique identifiers are provided that link the pledges to the payments. If identifiers are unavailable or unreliable, Client will need to provide a reliable method for matching

Functional Area	Description
	payments to pledges, otherwise they will not be linked in the conversion. The same process will be performed for installment pledges, soft credits and matching gifts.
Installments	An agreed upon schedule of payments to be made towards the balance of a Pledge.
Recognition Credits	The ability to credit one or more constituents when a constituent makes a donation.
Recognition Programs	A way to recognize donors based on their level of giving (e.g. Wall of Honor in a hospital).
Recognition Levels	The different levels a donor may belong to within a Recognition Program (i.e. Bronze, Silver, Gold).
Default Recogniton Credits	Allows a nonprofit to set up recognition credits based on the Household or on a Relationship type.
Schedules	Additional metadata about pledges (i.e. frequency, number installments).
Splits	A record that indicates revenue is allocated to specific fundraising purpose(s).
Recurring Gifts	An ongoing gift for a specific amount and scheduled at a specific time period.
Planned Giving	The process of giving a deferred gift, normally through a legal contract.
Accounts	Bank account records of a constituent. Normally used for EFT giving.
Credit Cards	Credit card records of a constituent used for credit card donations.
Wealth	Area of the Constituent record that allows you to detail the assets and estimated wealth of a constituent.
Write-Offs	The ability to reduce or zero-out a pledge balance.
Purposes/Designations	Record that defines the intention and use of the gift.
Modeling & Propensity	An integrated analytics tool that helps identify prospects most likely to give a gift and predict actions including planned and recurring gifts, membership renewals, and which constituent will become a major donor.
Events	A record that allows a nonprofit to create events as well as those constituents who attend them.
Prospects	A constituent that has been identified as a potential major donor or planned giver.
Correspondence	Record of correspondence between the Client and a constituent.
Staff	A constituency that denotes that the constituent works for the Client.
Marketing	Direct Marketing - the process to identify those constituents that have a higher propensity to give due to how they are contacted; and the tracking of the donations received. **Note —** Marketing data can be converted if it contains the following information: • Constituent or record ID representing marketing effort recipient • Package received by constituent • Segment the constituent was included in • Source code assigned to the constituent for that marketing effort • A unique identifier between revenue/response information to the marketing sent. This information must be provided for each marketing effort to be

Functional Area	Description
	converted. If segment information is not available, this information can be converted as Appeal Mailings rather than as Marketing Efforts.
Media Attachments	Attachments will convert where the file can be recognized as valid by the conversion engine for constituent attachments, event attachments, interaction attachments, and prospect plan attachments. Blackbaud cannot make any guarantees on which files will successfully convert.,
Media Links	Part of Documentation that allows links to URL pages (i.e. newspaper articles, Wikipedia, etc.).
Security	Site mappings and site hierarchy. Security roles assigned to users are not available through conversion.
Team Fundraising	The ability to help raise awareness and funds for a particular cause. A nonprofit can manage teams, team captains, and team fundraisers.
Tributes	Gifts made in honor or in memory of a constituent.
Volunteer	Functional area that allows the nonprofit to create Volunteer opportunities and track the constituents who volunteer for the opportunities.

5.6 Data Conversion Assumptions

Blackbaud will perform a direct transfer of thirty-two (32) Raiser's Edge databases and one (1) DonorQuest database into a single Blackbaud CRM instance. This transfer will be completed by a Blackbaud data analyst. The analyst will utilize the Blackbaud standard Raiser's Edge data map to convert records to Blackbaud CRM.

Legacy systems include 32 Raiser's Edge databases and 1 DonorQuest database. The eTapestry database and Excel spreadsheet are not included in the data conversion as they will be imported with support from Blackbaud consultants or re-keyed by Client resources into Blackbaud CRM. Any other databases that may be identified during the project will be imported or re-keyed by Client resources. If a full conversion of other databases identified during the project is deemed necessary, a Change Order will be required.

To help set clear expectations about the conversion process, the following assumptions have been taken into consideration:

Topic	Conversion Assumptions
Designation Hierarchy	Convert as single level direct transfer from **RE** fund records

- Blackbaud will directly transfer comparable data. Unless otherwise indicated in this SOW, the data will be converted "as is".
- Translations are used to map data to another functional area other than the indicated RE functional area. Translations will be limited to 500 hours inclusive of all Groups 1 through 4.
- Designation Hierarchy will be a single level direct transfer from The Raiser's Edge fund records.
- Education data will convert as code table entries and not to the academic catalog
- Revenue adjustment history and amendments are not included.
    - Adjustment details will convert as documentation on revenue records, and the revenue details will represent the post-adjustment amounts.
- Household records will convert based upon active spouse relationship records in The Raiser's Edge.
    - Basic contact information will be convertod on the household record

  - Addresses, Phones, Emails, Solicit Codes
- Default primary addressee and salutations will convert as standard defined formulas in CRM
  - Addressee and Salutation records from The Raiser's Edge will convert as text, custom name formats and will not be based upon Blackbaud CRM name format functions.
  - Blackbaud will not try to match Addressee/Salutations in the legacy system to Addressee/Salutation formula's in the Blackbaud CRM solution
- The Raiser's Edge has non-constituent records; Blackbaud CRM only has constituents. All non-constituent records, including individuals or organizations on relationships, will be created as a constituent in Blackbaud CRM and a relationship will be designated based on the data in The Raiser's Edge.
- If you have participants linked to an event but that participant record is not linked to the actual Raiser's Edge record a constituent record with a blank address will be created.
- Constituent records cannot convert to lists or selections.
- The Raiser's Edge allows gift records to split based upon Appeals, whereas Blackbaud CRM only allows one appeal per gift record. As a result, any gifts with split appeals will convert as a single gift linked to a single appeal record. The additional Appeal splits will be attached to the converted revenue record as attributes, and will be the responsibility of the customer to adjust the gifts post conversion.
- All revenue (excluding the past three fiscal years) will convert with a post status of 'Do Not Post', without GL distributions.
  - For the past three fiscal years, GL distributions will convert. Prior to conversion of GL distributions, the functional consultant must link designations to the CRM GL account structure
- Attachments will convert where the file can be recognized as valid by the conversion engine for constituent attachments, event attachments, interaction attachments, and prospect plan attachments. Blackbaud cannot make any guarantees on which files will successfully convert.
- Constituent soft credits will only convert where the data exists in The Raiser's Edge. New soft credits will not be created during conversion based on logic that exists in a configured CRM database.
- Data will convert to existing product functionality tables.
  - No customized data from The Raiser's Edge is included in this Statement of Work.
  - If supporting data exists in the legacy database, data will be converted into the Grateful Patient Solution as specified in Section 5.8.

5.7 ResearchPoint Conversion

Conversion of any ResearchPoint database is not included in this SOW. If conversion is desired, a Change Order will be required to complete the conversion.

ResearchPoint and WealthPoint data that already exists in the Raiser's Edge databases will be converted. RHMs that have imported ResearchPoint and WealthPoint data into existing Raiser's Edge databases must ensure data is up to date for accuracy of the conversion data.

Blackbaud and Client will initiate new wealth screening processes after Blackbaud CRM is live and all RHM data is converted.

5.8 Custom Solutions

This SOW is limited to the following custom solutions. If a custom solution and supporting information is not explicitly stated below, it is considered out of scope for this SOW and may require a change order if deemed a critical requirement.

Name	Type	Description
Grateful Patient Customization (RCP)	Customization	A packaged customization that provide fields to securely capture allowable PHI to meet business requirements and security policies.
Two (2) Custom Post to General Ledger Processes for Financial Edge and PeopleSoft Customization	Customization / Integration	Client will require a custom Post to GL process to integrate with the two different financial systems, including custom posting logic and output file format.
Auto File Downloader Customization (RCP)	Customization	Automation of data import and export processes for patient data and posting to the general ledger.

5.8.1 Grateful Patient Customization

Blackbaud has developed a "Packaged Customization" that will automate the import of Patient Data, Physician/Provider Referrals and Individuals and Organizations Related to the Patient. All information that can be captured in Blackbaud CRM adheres to the current HIPAA rules and allows customer to maintain the highest ethical and security standards possible. The packaged customization is flexible in that no information is required beyond the patient biographical data to successfully import a patient constituent. In addition to allowable PHI, the customization provides fields to capture allowable PHI elements that meet the business requirements and security policies of the organization implementing the customization. It is assumed that Partners Healthcare will implement the Grateful Patient Customization in its prepackaged form, but will impliment a change using Page Designer to make the Patient Tab visible on all Constituent records, regardless of whether or not there is associated Patient Data.

5.8.2 Two Custom Post to General Ledger Processes Customization

The Post to General Ledger processes identified in this SOW assume that Client will have a unified Chart of Accounts that each RHM uses as its standard. As per the Client and with Blackbaud's agreement, General Ledger Integration Design must be one of the first decisions made by Client's Philanthropy Program Steering Team. Trinity Health will have one Philanthropy Chart of Accounts whereby each RHM Foundation Chart of Account data will roll up into.

Client will require a custom Post to GL process to integrate with the the following financial systems:

- One (1) Financial Edge NXT
- One (1) PeopleSoft

Out of the box Segment Mappings

This SOW assumes that all RHMs General Ledger configurations will be completed using out-of-the-box functionality. Any custom mapping logic is out of scope and will require a Change Order.

Output File Format for Financial Edge

One (1) custom file format for the Financial Edge NXT will be delivered for Client. The solution assumes that Client will have one unified Chart of Accounts. The specific output file format will be specified during the Design Phase of the project.

Shared Output File Format for PeopleSoft

Blackbaud CRM does not output a PeopleSoft file format in the out-of-the-box Post to GL functionality, and one (1) custom file format will be delivered for Client. The solution assumes that Client will have one unified Chart of Accounts. The specific output file format will be specified during the Design Phase of the project.

5.8.3 Auto File Downloader / FTP Customization (RCP)

Data import and export processes may be automated, including the delivery of the Post to GL file(s) and the patient data file(s). Blackbaud has developed a "Packaged Customization" that provides the business process automation features needed to meet this need. The packaged customization includes three Business Process Connectors:

- *Auto file downloader:* This task automatically creates a file for a given Blackbaud CRM business process (e.g. Post to GL) and moves it to a specific location on the application server/shared drive.
  - This allows a user to skip having to download a file manually first before moving the file
- *FTP:* This task will provide functionality to transfer files between a remote FTP/SFTP site and Blackbaud CRM.
- *Zip files:* This process automatically zips (or unzips) files which are transferred to and from the Blackbaud CRM application server.

It is not anticipated that any updates to the packaged solution will be needed, and that the name format patterns for file name already included in the packaged solution will meet Clients' needs.

5.9 Adoption Readiness & Training Program Components

5.9.1 Adoption Readiness

Blackbaud integrates adoption readiness and change management into the overall implementation approach to assist Client's project leadership to assess the organizational readiness for change, understand the key impacts of the change, develop a strategy for consistently communicating the value of the project to all user segments, and preparing key stakeholders for managing the change that will result from the new technology and business processes. The project ultimately rests upon user adoption, and steps are taken to cultivate this, including:

Component	Description
Impact Analysis	Developed through interviews of key project stakeholders and an e-survey of the broad user community, this analysis identifies the organizational impact of the implementation, including: • Relevant business areas and their readiness for change • Risks and the specific mitigation plan for risks
Communication Workshop and Planning	The results of the Impact Analysis will be used to create an initial communications plan, which will be detailed in concert with the Client's Adoption Team during a workshop. It is the ultimate responsibility of the Adoption Team to execute on the communication plan. The Client will

Component	Description
	determine which staff is on the Adoption Team with Blackbaud's guidance.
Mid-Project Assessment	Approximately halfway through the project a survey will be conducted to assess the progress of the project, the communication plan, and any risks. The results of this work will allow for course corrections and risk intervention moving towards the end of the project.
Ongoing Support	Blackbaud Change Management resource will be available through monthly office hours to assist with challenges that arise throughout the project for coaching and mentoring through change issues. In addition, Blackbaud will identify and address risks related to end-user adoption and devise strategies to mitigate. This could be through additional communication or individual coaching sessions.
Pre-Go Live Workshop	Approximately one month before Go Live, the Blackbaud resource will engage in a refresher training of change management best practices and help plan the Go-Live communication and rollout.
Post-Go Live Survey and Look Forward	Approximately six months after Go Live, Blackbaud will assess satisfaction, adoption, and utilization of the solution via survey and interviews. Results of these will inform a session to report on the items and conduct "lessons learned," and next steps.

5.9.2 Training Program Components

The training program consists of several types of training, including

Training	Description
Page Designer Training	One (1) day of Blackbaud CRM Page Designer training to a maximum of eight (8) developers or system administrators. This training will prepare technical staff with the tools needed to maintain Blackbaud CRM system functionality and security. This training is also designed to allow developers to further customize and configure the application. • Explore the capabilities of Page Designer • Differentiate configuration versus customization • Permission features, Pages, Tabs, Sections • Actions, Data Lists, Context Links • Create/configure new Blackbaud CRM page • Configure Attribute Form Extensions
Data Outputs Training	One (1) day of custom report training for up to eight (8) developers utilizing Microsoft's SQL Server Reporting Services (SSRS) and Microsoft Excel® tools. Training will include extracting data using native Blackbaud CRM components (ad-hoc query, smart query, smart fields, selections, data lists, RSS feeds, KPIs, web dashboards, Excel exports) and building custom reports against the transactional database using SSRS. The SSRS portion of this class requires all students have the following components installed on their defined development workstations:

Training	Description
	• Blackbaud CRM • SDK • Microsoft Visual Studio 2008/2010 • SQL Server 2008/R2, 2012 configured with SSRS.
Report Writer Training	Blackbaud will provide three (3) days of custom report training in two different categories: **Report Writing Based on Transaction Database** Through this one (1) day course for up to twelve (12) participants, students will learn report building with Blackbaud CRM and SQL Server Reporting Services (SSRS). Reporting alternatives using out-of-the-box components are also discussed. Course content is focused mainly on leveraging SSRS to build and integrate custom reports into Blackbaud CRM. The following topics and exercises will be covered within this course. • Ad-hoc query-based reporting • Report model generated-based reporting • Traditional/Stored procedure-based reporting • Implementing selection-based reports • Report security model **Reports Writing Against the Data Warehouse** Two (2) days of training for up to twelve (12) participantswho will learn fundamental concepts, theory, and mechanics necessary to utilize a data warehouse. Course content focuses on the entities, schema, and best practices associated with the Blackbaud Data Warehouse solution, as well as addressing deployment, administration, customization, and multi-dimensional reporting using native CRM tools, SSRS, and Microsoft Excel. The following topics and exercises will be covered within this course. • Data warehousing fundamentals • Compare/contrast data warehouse with relational database theory. • Data warehouse architecture and integrating components (SSRS, SSIS, SSAS) • Deployment & Administration • Building multi-dimensional reports using OLAP Explorer, SSRS and Excel. • Building SSRS reports using the SQL Data Warehouse
Project Team Orientation	The purpose of this four (4) day orientation is to introduce and provide instruction on Blackbaud technology, implementation methodology, and training and support resources for the purposes of informing and equipping the project team in advance of project activities. The Blackbaud instructor along with Blackbaud project team members

Training	Description
	will prepare and deliver materials to orient Client project team members to the implementation including functional design, web design, change management, conversion, project collaboration site, custom solutions, and integrations.
Training Needs Analysis and Training Plan	Four (4) hour workshop with project team members, executives, managers, and key end users to assess actual organizational training and development needs. Final analysis includes strengths, weaknesses, opportunities, and threats/risks. Formal Training Plan will include a formal stakeholder Identification, Modes of Learning Recommendations, Courseware Recommendations, Training Scheduling Milestones, Sample Agendas, feedback programs
Project Team Training	Twelve (12) days of standard Blackbaud CRM training will be provided to the core project team and key staff members (up to twenty) prior to upcoming design cycles. Training will be conducted on a standard sample database provided by Blackbaud. Standard printed workbooks will be provided for up to twenty attendees.
BBIS Advanced Web Designer Training (Advanced Donation Form)	One (1) days of Advanced design training for up to twenty (20) participants includes the HTML, CSS, and design framework of the Advanced Donation form from an interactive designer's perspective. It is delivered in a facilitated workshop format and uses standard courseware with implemented Blackbaud Internet Solutions designs.
BBIS Online Build Training	Two (2) days total of online related training focused on training web administrators and system end users (up to twenty) to prepare team members for testing specific functions of the system related to online during business process testing and user acceptance testing. The two days will be split across three different sessions. These audiences will be trained on specific functionality of Blackbaud Internet Solutions and will learn the tools needed to test out the Blackbaud Internet Solutions website. One (1) day of training focused on sending email out of the Marketing and Communications tool within CRM. Including the review of the functions of the communication preferences form. Training to occur during the Business process testing cycle of the project in order to prepare end users for testing the solution. One (1) day of training will be split between two topics and the first half will be focused on the integration settings of Blackbaud Internet Solutions and transaction processing online data during the user accpetance testing cycle of the project. The second half will be focused on the Blackbaud Internet Solutions functional parts implemented as a part of the project.
Train the Trainer Training	Blackbaud will equip the Client's trainers with the necessary skills to effectively transfer knowledge to the end-user community. Seven (7) days of instruction will be provided for up to ten participants. Training components include software knowledge and knowledge transfer, followed by "teach backs." This training uses client-specific data.
Training Design	Blackbaud will complete six (6) days of onsite Training Design

Training	Description
	consultations to determine specific lesson objectives, develop training materials, and delivery timelines for each group of end users scheduled to receive training in advance of go-live. Additional days of training design may be purchased for development of post go-live training activities (e.g., onboarding new hires, periodic training session revisions, impact of business process changes, and upgrades)
Jumpstart Content Training	Jumpstart workbooks are a "do it yourself" solution for customers who have the staff to easily create and edit workbooks used during training. Customers receive electronic files of templatized standard product conceptual and "how-to" content for the functional areas included in their software solution. The content includes placeholders for suggested placement of graphics and activities and the customer owns the intellectual property rights to the file. Printing and upkeep of workbooks is the responsibility of the customer.
User Acceptance Testing Training	During eight (8) days of User Acceptance Tester (UAT) Training, participants are taught the knowledge and skills needed for testing product functionality during the testing phase of the project. In the case when Training Collateral (e.g., workbooks, job aids, slides) are available, they may be beta tested on UAT participants prior to use during final training. May include a "UAT Orientation" for new testers (delivered by Blackbaud or the client) session, if desired.

5.10 Software Version Scope

Blackbaud encourages its customers to be on the latest version of the Blackbaud CRM application software. If there is a publically available Blackbaud CRM upgrade that becomes available during the duration of this SOW, Blackbaud will recommend if and when the customer should choose to install the upgrade as a part of the implementation. If Client chooses to install the upgrade and change business processes or implement new business processes as a result of new features within the upgrade, including design, conversion, custom solutions, or reporting, a Change Order may be required to complete the additional work.

5.11 Language, Currency, Site Security and Location

The following languages shall be supported as part of this SOW.

- American English

The following currencies shall be supported as part of this SOW.

- US Dollars

Site Security will be implemented as a part of this SOW.

- Site(s) shall be used as a means to filter data only not as a means to secure data among Regional Health Ministries.

Trinity Health

Professional Services Statement of Work

Prepared by Bo Crader
May 13, 2015

blackbaud
your passion > our purpose

Exhibit A

Version Control Log

Date	Name	Description	Sections	Rev.
5.11.2015	Bo Crader	Document creation	All	1.0
5.11.2015	Susan McLaughlin	Review and reference to Blackbaud CRM SOW	All	1.1

Table of Contents

1 EXECUTIVE SUMMARY 3
1.1 Solution Overview 3
2 DELIVERABLES 4
2.1 Responsibility Matrix 4
2.2 Deliverables – TeamRaiser 4
2.3 Deliverables – Blackbaud CRM Integration 5
2.4 Deliverable Acceptance Procedures 6
3 ASSUMPTIONS & CLIENT RESPONSIBILITIES 7
3.1 General Assumptions & Responsibilities 7
3.2 SOW Specific Assumptions & Responsibilities 7
3.3 Software Version Scope 9
3.4 Language, Currency and Location 9
4 FEES, BILLING AND CHANGE ORDERS 10
4.1 Estimated Professional Services Fees 10
4.2 Billing Terms 10
4.3 Change Orders 11
4.4 Expiration of Services 11
4.5 Cancellation Policy 11
5 SOLUTION COMPONENTS – TeamRaiser 12
6 SOLUTION COMPONENTS – Blackbaud CRM Integration 13
6.1 Supported Data Integrations 13
6.2 LO-Blackbaud CRM Integration Custom Solution 13

Exhibit A

1 EXECUTIVE SUMMARY

This Statement of Work (SOW) outlines the high-level solution, deliverables and estimated costs required to implement TeamRaiser and a custom data integration between Luminate Online (LO) and Blackbaud CRM (BBCRM) for Trinity Health.

This SOW is subject to the terms and conditions of the Master Services and Support Agreement. Throughout this document, Trinity Health will be referred to as "Client" and Blackbaud Professional Services as "Blackbaud."

1.1 Solution Overview

1.1.1 TeamRaiser

Blackbaud will implement TeamRaiser to support one of Client's event fundraising programs. A Blackbaud CRM consultant will be involved in the TeamRaiser implementation component to ensure continuity with the Blackbaud CRM implementation and its dependent business processes. Please refer to the separate Blackbaud CRM Professional Services Statement of Work (dated April 10, 2015). Because of the dependencies between the Blackbaud CRM and TeamRaiser implementations, this SOW assumes the Engagement Manager for the Blackbaud CRM implementation will provide overarching project management for the Team Raiser implementation.

1.1.2 Blackbaud CRM Integration

Blackbaud will implement a "best practice" data integration between Client's Luminate Online (LO) and Blackbaud CRM (BBCRM) instances. **Note: Luminate Online is the platform upon which enables TeamRaiser event fundraising.**

This packaged design provides a standard set of capabilities but can be configured for Client's specific requirements. At a high level, the integration provides the following capabilities:

- Pre-packaged, "baseline / standard" BBCRM customization, supported by Blackbaud
- Near-real-time sync via Web services APIs
- Constituents bi-directional sync
- Events, event registrations, and revenue unidirectional from LO to BBCRM

Blackbaud and Client will collaborate on the timing, scheduling, and resource staffing of work in this SOW.

2 DELIVERABLES

2.1 Responsibility Matrix

A responsibility assignment matrix, (also known as RACI matrix) describes the Deliverables and each party's respective role relating to each Deliverable. Deliverables are those items specifically identified as a "Deliverable" in this SOW. The table below provides an overview of categories of responsibility.

Category	Definition
Responsible (R)	The party who does the work to achieve the Deliverable. At least one party is assigned as the responsible party, although other parties are delegated to assist as required.
Accountable (A)	The party ultimately answerable for the correct and thorough completion of the Deliverable, and the one who delegates the work to responsible parties. An accountable party must sign off (approve) on work that the responsible party provides. One accountable party is assigned for each Deliverable.
Consulted (C)	The party who is consulted before a decision or action is taken. Consulted parties are not expected to produce the Deliverable, but instead will provide general advice concerning the Deliverable.
Informed (I)	Those parties who are kept up-to-date on progress, often only on completion of the Deliverable.

2.2 Deliverables – TeamRaiser

Deliverable	Description	Client	Blackbaud
Project Plan	Project Schedule built in MS Project indicating milestone dates, dependencies, and responsible parties. Once both parties have signed off on Project Plan, changes to plan will require a change order. *Note: Because this SOW is executed in line with the larger Blackbaud CRM implementation SOW and in consideration of project dependencies, a single project plan will be used to manage both projects.*	C	A, R
Production Environment Configuration	Blackbaud will conduct the build-out of Luminate Online in Client's production instance of Luminate Online.	I	A, R
Test Plan	Documentation of what will be tested, how it will be tested, and what the expected outcome of the tests will be.	A, I,C	R
PageWrapper	Configuration of a single (1) PageWrapper based on an existing website design provided to Blackbaud by Client.	C, I	A, R
TeamRaiser Event	Creation of a single TeamRaiser event and correlating donation form to support the Client's peer-to-peer fundraising program.	C, I	R, A

Deliverable	Description	Client	Blackbaud
UAT Plan	Creation of User Acceptance Test Plan for all Deliverables	A, R	C, I
UAT Report	Client will perform User Acceptance testing and provide a report of their results to Blackbaud	A,R	C

2.3 Deliverables – Blackbaud CRM Integration

Deliverable	Description	Client	Blackbaud

Integration Design	Following a prescriptive process, Blackbaud will conduct detailed discovery of data exchange requirements. The assessment will address:
	• Data map and any custom mapping requirements identified in business process design
	• Data transformation requirements / business rules
	• Other custom requirements not presently scoped (for which additional hours may be required to bring into scope)
	• Recurring data exchange workflow
	• Constituent data deduplication and equalization options
	  o Name only
	  o Name + email
	  o Name + address
	  o Custom rules (additional hours would be required)
	
	This process is best conducted after Client's project team has made preliminary decisions about cross-platform business process requirements between Luminate Online and Blackbaud CRM. Note: custom mapping requirements may require a Change Order.
		C	A,R

Data Map	Blackbaud will supply a "best practice" data map for Client's review and approval. Client's custom fields may be mapped through the standard integration via configuration. Beyond this limited flexibility to encompass client-specific needs, material changes to the prescriptive data map or to the direction of data flow between systems is *not recommended* and will require a Change Order.	C	A,R
Constituent Data Equalization	If required, Blackbaud will provide and execute equalization logic for synchronization of constituents between LO and BBCRM at the time of LO initial launch. Note: Because Client is implementing a new instance of TeamRaiser and with no existing constituents, Constituent Data Equalization is not required.	C	A,R

Deliverable	Description	Client	Blackbaud
Data Exchange Baseline Solution	The data exchange will address all the data flows described in Custom Solutions, below. Operation of the data exchange will be managed via scheduled and on demand processes. The solution will also include Blackbaud CRM UI enhancements to surface TeamRaiser data which is brought into Blackbaud CRM. Note: Certain additional integration functionality is possible "out of the box" with standard functionality in Blackbaud CRM version 3.0 Service Pack 8 and above when deployed with Blackbaud Data Warehouse (BBDW). Client may choose to configure this functionality as well, although not all customers require this integration between LO and the BBDW.	I	A,R
Interface Testing	Blackbaud will support Client in testing the operability and effectiveness of the integration. Standard testing support includes initial testing prior to delivery of the installed customization to Client, guidance on how to efficiently sequence testing steps, and resolution of issues reported by Client. Client is responsible for organizing their testing effort and managing issues reporting, tracking and closure.	R	A, C
Data Exchange Launch	At the time of final cutover, Blackbaud will configure the integration for live use, equalize constituents if necessary, instruct the client how to administer recurring operation of the data integration, and provide up to 20 hours of post launch stabilization assistance.	I	A,R

2.4 Deliverable Acceptance Procedures

The acceptance criteria and procedures for Deliverables apply only to Deliverables for which Blackbaud has been designated as the "R" party. The provisions of the Agreement are supplemented by the Deliverable acceptance provision below.

- Blackbaud will make available Deliverable to Client for review and acceptance
- Client will provide an adequate number of resources to review Deliverable to confirm conformity in all material respects based upon mutually agreed requirements and specifications developed during this Project
- Client will provide written notice of acceptance or rejection within ten (10) business days of notification of delivery. Deliverables which are not rejected by Client within the above time period shall be deemed accepted.

3 ASSUMPTIONS & CLIENT RESPONSIBILITIES

The performance of Services, timing, resources and fees associated with this SOW are based on the assumptions and Client responsibilities set forth below. Should any of these assumptions not be fully realized or should Client fail to timely perform its responsibilities below and elsewhere in this SOW, a Change Order shall be required resulting in adjustment of the fees, expenses, and schedule associated with this SOW.

3.1 General Assumptions & Responsibilities

- Please refer to Section 3.1 in the Blackbaud CRM Statement of Work (dated April 10, 2015) for the General Assumptions & Responsibilities that apply to Blackbaud implementations. The Blackbaud CRM Statement of Work and the Luminate Online TeamRaiser Statement of Work will be implemented simultaneously with a coordinated and combined project plan. All general assumptions and responsibilities set forth in the Blackbaud CRM Statement of Work apply to the Luminate Online TeamRaiser Statement of Work.

3.2 SOW Specific Assumptions & Responsibilities

3.2.1 TeamRaiser

- This service includes usage of the standard Luminate Online and TeamRaiser product functionality and templates; any customizations will require a separate statement of work and potential ongoing maintenance fees. For purposes of greater clarity, no customizations are included in this SOW.
- Client will provide all necessary design and de-duped data elements for the Application Service pages, including the PageWrapper design and images, according to the then-current version of the Design Guidelines.
- Blackbaud will make reasonable efforts to re-create styles and functionality on Client's current site, but in some cases, this may be limited by platform constraints.
- Client will maintain and revise stationery and page wrapper beyond one round of revisions.
- Multi-lingual content may be supported by certain Application Services; however, this Service does not include services related to developing and supporting multi-lingual content pages.
- Client must supply content for TeamRaiser content pages, auto-responders, suggested messages, email campaign content, images, etc.
- All work effort to deploy TeamRaiser under this SOW will be provided on a time and materials basis.
- All work effort in this SOW will be performed remotely unless specifically indicated otherwise in this SOW.
- Client will use standard Merchant Account setup with Blackbaud Merchant Services (BBMS) as indicated on Order Form.
- Domain name will be "*ShortName*.convio.net" where "ShortName" indicates a subdomain name provided by Client. If Client would like to use a dedicated domain name ("Client.org" or "subdomain.client.org") the appropriate subscription must be included on Client's Order Form.

3.2.2 Responsive Page Wrapper

Subject to the limitations specified herein, Blackbaud will engage with the Client to implement one (1) Page Wrapper that dynamically adjusts to one of four screen resolutions: 320px, 480px, 768px, and 992px.

Client Responsibilities include the following:

- Unless indicated specifically otherwise within this SOW, all services will be provided using the standard Luminate Online toolset without customizatoins or custom data services.

- Unless bundled with Blackbaud design services, the Client will provide final design assets in an organized fashion at the start of the project. The designs will adhere to the then-current version of the Blackbaud Design Guidelines, and the Client responsible for any licensing in association with photo usage fees.
- Electronic delivery of the design will be in the form of one layered Photoshop (PSD) file in actual dimensions or one layered Illustrator (EPS) file with vector based art for each of the four screen sizes. Additional graphics may be supplied in the highest possible resolutions within the following formats: PSD, PNG, TIF, TIFF, JPG, GIF.
- Client is responsible for the creation of new content using this Page Wrapper and/or applying it to any existing content or campaigns. This includes structuring content that will be embedded within the wrapper to be responsive.
- Blackbaud will only apply up to 30 hours towards the completion of services related to creation of a Responsive PageWrapper under this SOW.
- No rounds of revision are included. Changes to the design after it is delivered to Blackbaud will impact the Project timeline and result in additional fees.
- Solution will be tested against the then-current versions of mobile browsers supported by the Application Services. Requests to address additional browser incompatibilities will be considered billable work and may require an additional statement of work.
- Price and timeline are contingent on confirmation of requirements at project kick off. Designs that use complex interaction paradigms may result in an increase in Project timeline and additional fees. Any change requests from this original scope agreement will be scoped and estimated for cost and time separately.
- If this Page Wrapper is applied to Application Pages that contain non-responsive content, that content may not render responsively.

3.2.3 Blackbaud CRM Integration

This SOW assumes the deployment of the pre-packaged, "baseline / standard" Blackbaud CRM integration:

- Development is already complete; no enhancements to the prepackaged integration solution or to existing Blackbaud CRM or LO product functionality are scoped.
- Blackbaud CRM and LO do not have identical data models; the integration employs "work around" solutions and a data governance model to address critical product differences (e.g. organizational giving, soft credits).
- For reference, this SOW does not include a Single Sign-On (SSO) between BBIS and LO.

LO implementation will follow Blackbaud best practice recommendations for integrated business process design

- Blackbaud will provide a data map, best practices guidance document and sample use/test cases describing the intended methods of using of this integration.
- Specific field mapping requirements are normal and allowed, but extra features or deviations from the integration data governance model could involve material extra cost

The baseline package integration as deployed by Blackbaud for Client will be supported under the terms found at maintenance.blackbaud.com until such time as a productized integration is created. If a newer version of the baseline package is released and/or feature enhancements are added to the Covered Software, the cost to adopt the new version or features sets will not be covered under the scope of support and may require a Services implementation engagement.

Blackbaud recommends Client purchase a LO Test environment for post-launch use in maintaining and enhancing their LO system and the Blackbaud CRM integration.

- An ongoing LO Test environment is provided through a subscription model and must be purchased by Client via an Order Form. An ongoing LO Test environment is not included in this SOW.

- Client will install the integration if a test environment is purchased

This SOW does not include work effort for migration of recurring gifts. Recurring gifts will be set up and managed through BBIS as defined in the Blackbaud CRM Statement of Work dated April 10, 2015.

3.3 Software Version Scope

The scope of this SOW is limited to the versions of application and other software identified below. No upgrade will occur of any of this software to a different version by either party prior to the installation of each release into production.

- Blackbaud CRM version 3.0 Service Pack 8 and above, or Blackbaud CRM version 4.0
- Luminate Online currently released version

3.4 Language, Currency and Location

The following languages shall be supported as part of this SOW.

- American English

The following currencies shall be supported as part of this SOW.

- US Dollars

All Services under this SOW shall be provided from the following locations

- Blackbaud offices located in the United States
- The homes or home offices of the Blackbaud consultants assigned to the Project

4 FEES, BILLING AND CHANGE ORDERS

4.1 Estimated Professional Services Fees

Time & Materials Services Fees					
Service Description	Hours	Rate	Fee	SKU	Billing Terms
Web Development	122	$200.00	$24,400.00	WDLOTM	T&M
Project Management	46	$200.00	$9,200.00	PMLOTM	T&M
Quality Assurance	16	$200.00	$3,200.00	QALOTM	T&M
Training (Ed Services)	12	$200.00	$2,400.00	TRNLOTM	T&M
LO Integration Packaged Deployment	1	$32,000.00	$32,000.00	ECSGEAPFPE	FP - Scheduled
T&M Totals:	213		$71,200		
Discount:			($3,700)		
Total After Discount:			$67,500		

4.2 Billing Terms

Billing Term	Description
T&M	The professional services described here are provided on a time-and-materials (T&M) basis only. The estimate(s) cited above represents an estimate only and does not reflect any binding obligation for Blackbaud to complete those services within the estimated time or cost. Any required changes to the estimates will be processed with approval as defined in the Change Order section of this agreement. Upon signing and returning the Agreement to Purchase, Blackbaud shall invoice Client for services rendered based on the number of hours expended by Blackbaud. These fees do not include any travel-related expenses.
FP Scheduled	The services described here are billed on a fixed price basis. Upon receipt of the signed Agreement to Purchase, invoices will be generated and paid in accordance with the following schedule: 50% due upon signing 50% upon completion of the engagement These fees do not include any travel-related expenses.

4.3 Change Orders

Blackbaud shall perform the services specified in this SOW. Any other services or changes identified by the parties will require a duly executed Change Order. If the parties mutually agree to change this SOW, then, Blackbaud will create a Change Order documenting the change in Statement of Work, additional (or exchanged) services to be delivered and resources required, any changes to the project plan and/or deliverable dates (if applicable), and additional estimated fees (if applicable).

Both parties must properly execute the change order before any resources will be assigned or any additional/changed services will be performed. Any properly executed Change Order is subject to the terms of the Master Software and Services Agreement and this SOW.

4.4 Expiration of Services

If, (I) within one year of execution of the SOW, the Client has not scheduled any work to be performed, or (ii) if the Client has scheduled work to be performed, but due to the unavailability of the Client such work has not commenced within six (6) months of being scheduled, the SOW will be deemed to be terminated by the Client and any fees paid in connection with this SOW shall be retained by Blackbaud and applied toward a cancellation fee.

Prepaid services not scheduled within 18 months shall be deemed expired and any fees paid in connection with this service shall be retained by Blackbaud.

4.5 Cancellation Policy

In the event services are scheduled pursuant to this SOW and the Client cancels or postpones with less than ten (10) business days' notice, the Client shall pay for the committed hours at the applicable rates plus any out of pocket expenses incurred.

5 SOLUTION COMPONENTS – TeamRaiser

Component	Notes
Visual Design / User Experience	• 1 Responsive Page Wrapper based on Client's current website design to be provided to Blackbaud by Client, to be used across all pages. • Note: Client will be responsive for providing Responsive breakpoint components of PageWrapper design, as well as the standard desktop design
TeamRaiser	• Configuration of one (1) TeamRaiser for one of Client's event fundraising programs (to be named), using the Page Wrapper (visual design) implemented under this SOW. • Setup of the TeamRaiser event will use standard functionality only (no customizations) and will include a Home Page, participant center, related pages, and autoresponder messaging based on content provided by Client. • Configuration of one (1) TeamRaiser event registration, including participation types, registration upsells, waiver, additional questions requested/required at time of registration. • Initial set up of auto responder messages (up to 15) associated with TeamRaiser event registration. • Initial set up of customized suggested messages for participant race center. Initial set up of TeamRaiser pages (up to 18) includes registration steps, Race Center home page, default personal page. • Creation of tasks/group to capture TeamRaiser event team captains and participants. • One (1) round of revisions for all aspects of TeamRaiser.

6 SOLUTION COMPONENTS – Blackbaud CRM Integration

This project will begin with a baseline LO integration with Blackbaud CRM (BBCRM). Blackbaud will provide a temporary LO test environment for the implementation. As noted in Section 3.2.3, Client may consider the purchase of a permanent LO Test environment. Client is responsible for designating one of the Blackbaud-hosted, non-Production BBCRM environments to pair with the LO test environment for testing purposes.

- Blackbaud will install and assist Client in testing the integration solution, including a one-time data equalization, if needed.
- Blackbaud will install the integration solution in Client's LO and BBCRM Production environments for launch.
- Blackbaud will re-equalize the constituents in Production, launch the sync, and assist Client with post launch stabilization action items as needed.

6.1 Supported Data Integrations

Blackbaud Professional Services will implement our custom, "best practice" data integration between Client's Luminate Online (LO) and Blackbaud CRM (BBCRM) instances. This prepackaged design provides a standard set of capabilities and will be incrementally customized for Client's specific requirements.

Luminate Online Functional Area	Pre-packaged Data Integration Scope	Synch Direction
Constituent Management	Constituent biographical data, postal addresses, phones and email	2-ways between LO and BBCRM
Email interactions and preferences	LO email interactions and email interests	1-way from LO to BBDW; BBCRM version 4.0 and above can query BBDW for this data when needed
Constituent merges	BBCRM will be the system in which duplicate constituents are managed; LO will execute merges as instructed by BBCRM.	1-way from BBCRM to LO
TeamRaiser	New and changed TeamRaiser Events New and returning TeamRaiser teams, including updates to these teams New TeamRaiser event registrations New TeamRaiser event donations	1-way LO to BBCRM
Surveys	Survey questions and responses	1-way LO to BBCRM

The prepackaged solution may support additional LO data exchange with BBCRM beyond those areas listed above. Client may implement additional integrations themselves or with Blackbaud's help. A Change Order may be required if Blackbaud is needed to deploy additional integration business processes.

6.2 LO-Blackbaud CRM Integration Custom Solution

This SOW is limited to the following custom solution. If a custom solution and supporting information is not explicitly stated below, it is considered out of scope for this SOW and may require a change order if deemed a critical requirement.

Blackbaud Professional Services will implement version 2.5 of the best practice data integration between Client's Luminate Online (LO) and Blackbaud CRM (BBCRM) instances. This prepackaged design provides a standard set of capabilities and can be incrementally customized for Client's specific requirements.

6.2.1 What the Interface Will Do

If required, an initial, equalization process will be conducted when the interface is first deployed. The precise approach for the equalization will be decided with Client based on the client-specific needs and options determined from Blackbaud's best practice experience.

Thereafter a recurring, scheduled data exchange will take place in near real time[1] to synchronize the data which is new or has changed.

6.2.1.1 Prerequisites / Conditions:

For best results with the prepackaged baseline integration, Blackbaud recommends that Client

- Turn off address updaters in LO so that BBCRM addresses are what LO keeps
- Turn off automated LO welcome message for constituents introduced via data synch
- Require constituent record inactivation flags to be set/reset in BBCRM and do not allow inactive LO records to be downloaded to BBCRM
- Commit CRM batches automatically (with the possible exception of revenue; although the client can configure the template to do so anyway); and allow the integration to generate BBCRM exception batches for subsequent, manual resolution.

The following data synchronizations will occur when the exchange is triggered (in order of operation)

6.2.1.2 People

- Duplicate management will be managed in BBCRM with upload of duplicate resolution outcomes to LO
- Import of constituent data to LO from CRM - new or modified constituents and contact information
- Export of constituent data from LO to CRM - new or modified constituents and contact information

6.2.1.3 Events

- New and changed TeamRaiser events, from LO to CRM (the event data that has a natural place to exist in BBCRM, which is not everything about the TeamRaiser).

6.2.1.4 Event Registrations

- Team Raiser event registrations, which will import from LO to a customized CRM event registrant batch.
- The team information will be included. A UI customization will facilitate this in BBCRM by linking the Team Appeal to Team Group, and surfacing a hyperlink for the Team record on the Event to the associated Constituent Group.
- Changes to team roles and membership, from LO to BBCRM.

6.2.1.5 Money

- Team Raiser gifts, from LO to CRM
    - Registration fees
    - Gifts to a participant's event (with recognition credit applied to the participant)
    - Additional gifts to the event in general or to event teams.

[1] For most data. Near real time data exchange will often occur within seconds or minutes after data entry in the source system but depends on how frequently the client chooses to schedule synchronization and on the amount of data being entered into each system. There is no upper limit to how long it may take for the integration to recover from an unusual peak in data entry.

6.2.2 What the Interface Won't Do

The following are exclusions from the data exchange design. In some cases, a Change Order with additional hours could address these exclusions:

- The interface will not respect clients' use of Luminate Online Multi Center and BBCRM Site Security as methods to restrict access to records based on user security profiles – this can be completed with additionally scoped services.
- Data needed in BBCRM only for reporting or marketing segmentation purposes may not be included. Client should consider porting it directly into their data warehouse via conventional ETL processes.
- Soft recognition credit will be assigned to a TeamRaiser event participant when a donation is made to that participant's TeamRaiser. However in other respects, Luminate Online does not have the concept of soft recognition credit. All other soft credits associated with revenue entered into Luminate Online need to be maintained in BBCRM.
- The data exchange will not handle Refunds processed in Luminate Online. Client should plan to do this manually as an export from LO and then enter them manually into BBCRM or via a custom BBCRM batch.
- Although constituent data is a two-way synch, data about events, event registrations and revenue will not be pushed to LO if entered in BBCRM. If the data needs to surface online, Client should plan to enter it initially in LO and then the data exchange will bring it down into BBCRM.
- PGP Encryption cannot be done in an automated sync interface.
- The data exchange does not sync with BBIS or provide Single Sign On (SSO) capability between LO and BBIS.
- The batch data exchange does not address interoperability from the user's perspective other than in the pre-built BBCRM UI enhancements concerning team data.
- Although the BBCRM Constituent Lookup ID limit is 100 characters; LO member ID is 32 characters max. Client needs to keep this in mind during legacy data conversion.

blackbaud
your passion ▸ our purpose

Order Form

The fees and terms quoted in this Order Form ("Order Form") are valid until 06/30/2015. This Order Form and the purchases set forth herein are subject to and governed by the Master Services Agreement ("MSA") dated June 17th, 2015 and by signing this Order Form you agree to be bound by the MSA.

Client Information

Issued to:
Trinity Health

Mailing address:
20555 Victor Parkway
Livonia, MI 48152

Principal contact:
Philip Mccorkle

Principal contact email:
philip.mccorkle@trinity-health.org

Net Terms:
NT45

Bill to:
Trinity Health

Billing address:
20555 Victor Parkway
Livonia, MI 48152

Billing contact:
Mike Mrkich

Billing contact email:
michael.mrkich@trinity-health.org

Order Form No.:
Q-00072335

Order Summary

	Year One Fee	Year Two Fee	Year Three Fee
Subscriptions	$420,000	$420,000	$420,000
Services	$2,374,900		
Totals	$2,794,900	$420,000	$420,000
Grand Total	$3,634,900		

Signatures

IN WITNESS WHEREOF, the parties have caused this Order Form to be executed by their duly authorized representatives.

AGREED:

Client : **CLIENT**	**Blackbaud Authorize Signature**
By :	
Name : Miles B. Shipley	Name: Brian E. Boruff
Title : CFO	Title: President, Enterprise Business Unit
Date : 6.18.15 (*Effective Date)	Date: 06/15/2015

Exhibit A

Services

Type	List Price	Discount	Discounted Price	Total Contracted Value	Term	Billing
CRM Consulting Services	$2,595,825	$288,425	$2,307,400	$2,307,400	N/A	See SOW
TeamRaiser Services	$71,200	$3,700	$67,500	$67,500	N/A	See SOW

Subscriptions

Type	List Price	Discount	Discounted Price	Total Contracted Value	Term	Billing
Blackbaud CRM – 150 concurrent users	$420,000	$0	$420,000	$1,260,000	36	$420,000 Annual upon signing
CRM Hosting Annual Fee	$0	$0	$0	$0	36	N/A
TeamRaiser	$4,500	$4,500	$0	$0	36	N/A

Conference

Type	List Price	Discount	Discounted Price	Total Contracted Value	Term	Billing
Blackbaud Conference for Non-Profits – Two Registrations	$1,900	$1,900	$0	$0	N/A	N/A

Transaction Fees

5% Per Team Raiser Transaction, per month

General Terms

Fees are in **USD**

State Sales Tax Exemption Certificates

Does the State in which you are making this purchase provide a sales tax exemption for your organization?

{{*Tax_es_:signer1:dropdown(options="Yes,No ", values="Tax Exempt,Taxable ")}}

If you answer "Yes" to this question, Blackbaud is required to have a copy of the "State issued sales tax exemption certificate" for your organization on file. Please note Blackbaud cannot accept an IRS or State issued letter for 501(c)(3) status, entity incorporation, or income / franchise tax exemption as these are not acceptable forms for sales tax exemption purposes. You will receive a separate email link from Blackbaud@teamscert.com which will provide detailed instructions about how to submit your sales tax exemption form. If you do not submit a valid sales tax exemption form within 5 business days from the initial email contact, your organization will be treated as not tax exempt.

If you cannot provide a "State issued sales tax exemption certificate" or your State does not have a sales tax, please answer "No" to this question.

If you answer "No" to this question or you do not provide a valid sales tax exemption form with the 5 business day time period noted above, you will not receive a credit for sales tax billed prior to receipt of a valid exemption certificate.

Sales Tax on Products Purchased

Sales tax will only be charged on this order if the items purchased are subject to tax, depending on State law. For example, state sales tax rules vary depending on the delivery method of the software.

If you must remit sales tax to your vendor but can later claim a refund with your State, please answer "No" to this question. Blackbaud must still charge sales tax on this order (if applicable) even though you may ultimately receive a refund of the sales tax.

Payment Services

Processing of online financial transactions through the Blackbaud offerings purchased on this Order Form is subject to and governed by the http://www.blackbaud.com/files/bbms/bbpstc.pdf and attached herein as Attachment 1 and by signing this Order Form you agree to be bound by the BBPS Addendum.

Professional Services

The services to be provided are described in the accompanying Statement of Work.

Subscriptions

The subscription charges listed on this Order Form are for this purchase only. If you currently receive a subscription from Blackbaud, the above charges may be added to those and prorated to coincide with your current maintenance renewal date.

The term of your Subscription commences on the day you execute this Order Form and continues for the duration set forth in the applicable line item above. Subscriptions are billed according to the schedule set forth above.

Trinity Health can purchase additional users for BBCRM for $2800 per user for three years from signature of order form.

The default maximum storage space for Blackbaud CRM is 9TB.
Blackbaud will monitor disk usage on a regular basis, and will increase your organization's disk space allocation in TB increments with an increase of $12,000 annually when disk utilization exceeds the next pending threshold.

Blackbaud Payment Services
Addendum

1. Blackbaud Payment Services ("BBPS").

BBPS will collect, transmit, and store credit card data for processing of payments with Blackbaud approved Payment Gateways and Payment Processors (as such terms are defined in Section 2. BBPS Options below) in accordance with the Payment Card Industry Data Security Standard (**"PCI DSS"**). Client will retain "tokens" in its product application database to simplify processing through Payment Gateways. Blackbaud will provide BBPS in accordance with the service levels described in "Exhibit C, BBPS Service Levels". Blackbaud will use the cardholder and online financial transactions data of Client (**"Data"**) only in the performance of BBPS; provided, however, Blackbaud may use the Data (in an aggregate form) combined with the data of other Blackbaud clients for statistical analysis and reporting.

2. BBPS Options.

A credit card payment "gateway" services provider (a **"Payment Gateway"**) and a credit card payment processor (a **"Payment Processor"**) are required to process credit card and bank card transactions. Client processing payments with BBPS agrees to purchase one or more of the following BBPS options:

a) Blackbaud Merchant Services ("BBMS"): Blackbaud provides contracted services for a Payment Gateway and Payment Processors in accordance with "Exhibit A, BBMS".

or

b) Third-Party Merchant Services with Blackbaud Gateway Interconnect Option (**"Blackbaud Gateway Interconnect Option"**): Blackbaud provides a payment vaulting/gateway interconnect to an approved third-party Payment Gateway and supported third-party Payment Processors in accordance with "Exhibit B, Third-Party Merchant Services with Blackbaud Gateway Interconnect Option". Client is responsible for directly engaging and contracting with a Blackbaud approved Payment Gateway and Payment Processor.

3. Client Responsibilities.

To use BBPS, Client must:

a) Purchase either BBMS or Blackbaud Gateway Interconnect Option and, in each case, establish and maintain a merchant account for payment processing for the Blackbaud Products set forth in the Agreement.

b) Maintain active status in a Blackbaud Software Maintenance and Support Program for purchased application software using BBPS which includes the maintenance and support of Client's selected BBPS option.

c) Identify to Blackbaud (by providing name and contact information including electronic mail address) the "Primary Contact" for BBPS (i) who has the authority to make BBPS related requests including release of Client data, restoration of data, and other configuration changes and (ii) with whom Blackbaud will communicate on BBPS related matters including maintenance notifications. If a Primary Contact is not properly identified by Client to Blackbaud, Blackbaud shall have the right to deem Client's contact for this Agreement (or an individual

previously identified by Client to Blackbaud, if applicable) as Client's "Primary Contact".

d) Administer security within the product applications (*e.g.*, granting of rights to a user for a specific form in the applications). Client is also responsible for maintaining its users' desktops and providing users with network access to BBPS.

e) Provide connectivity and secure access to the Internet for Client's locations to provide adequate access from Client's Blackbaud Products or to BBPS's secure platform.

f) Use commercially reasonable precautions to ensure security for integration between applications at the Client site and BBPS.

g) Advise Blackbaud in advance of any changes to Client's operations, banking relationships, Primary Contact, or other information that would require a change in the support, operation, or configuration of the hosted applications.

h) (i) Use BBPS only for its own legitimate business purposes, (ii) not use BBPS for load testing, and (iii) not sell or provide, directly or indirectly, any portion of BBPS to any third party.

i) Maintain PCI DSS compliance.

j) Ensure that any Client's products or services (excluding any Blackbaud Products) used in conjunction with BBPS do not infringe any intellectual property rights of any third party.

k) Comply with all applicable laws, rules, and regulations including laws regarding privacy and protection of consumer data and comply with the Visa Cardholder Information Security Program and all other applicable rules of card associations, including American Express®, MasterCard®, and Visa®.

l) Maintain and observe all commercially reasonable security measures to protect its systems, including the Blackbaud Software and the data contained therein, from unauthorized control, tampering, or other unauthorized access, including compliance with the Visa Cardholder Information Security Program, if applicable. For the purposes of this Section, "**Blackbaud Software**" means the computer systems operated by or on behalf of Client that capture or store end user data, or that transmits end user data to the Payment Gateway.

m) Provide all disclosures to and obtain all consents from each end user, in each case as required by the card associations and applicable law, prior to transmitting information relating to such end user to BBPS and the relevant Payment Gateway.

4. Acceptable Use Policy.

Use of BBPS is subject to Blackbaud's Acceptable Use Policy located at http://www.blackbaud.com/aupolicy.aspx, as amended from time to time.

5. Term and Termination of BBPS.

BBPS shall be provided during the term of the Agreement. Each of Blackbaud and Client may terminate BBPS for any or no reason at any time upon 30 days' written notice to the other party. Upon such termination, Client may make written request to Blackbaud for available stored Data. If Blackbaud provides such Data to Client, Client will be required to (a) accept terms associated with the retrieval and delivery of such Data including any security procedures which Blackbaud determines are required by PCI DSS and (b) be responsible for paying to Blackbaud the cost of such services (on a time and material basis). Client shall be responsible for any and all chargebacks, refunds, and any other fees associated with payment services following termination of BBPS. Client may reinstate BBPS but may incur additional fees to do so.

6. Change, Replacement, or Termination of Third-Party Payment Gateway.

Blackbaud reserves the right to change, replace, or terminate the services of any third-party Payment Gateway upon 30 days' notice to Client. In the event of replacement of a Payment Gateway, Client understands and agrees that it may be required to execute additional terms and conditions associated with such a replacement.

7. PCI Compliance Indemnity; Limitation of Liability.

The following provisions shall apply in addition to the terms set forth in Section 10 of the Agreement: (a) Blackbaud shall indemnify and defend

Exhibit A

Client against any third-party claim arising from Blackbaud's failure to maintain BBPS in compliance with PCI DSS. This Section states the entire liability of Blackbaud with respect to any such third-party claim. Client shall give Blackbaud prompt written notice of any such claims for indemnification and Client agrees to relinquish control of defending any such claim to Blackbaud, including the right to settle. Subject to Section 10.a. of the Agreement, the maximum liability of Blackbaud to Client for the indemnification obligations set forth in this Section is $1,000,000. (b) For the avoidance of doubt, Blackbaud shall not be liable to Client, whether by way of indemnity or by reason of breach of contract or in tort, or on any other legal or equitable basis, for the loss of any donations by donors to Client that may be suffered by Client. The parties agree that any such losses are indirect or consequential damages, liability for which is specifically excluded under Section 10.a. of the Agreement.

8. Client is not a Third Party Beneficiary.

Nothing in this Addendum, express or implied, is intended to or shall confer to Client or any other person any right, benefit, or remedy of any nature whatsoever under Blackbaud's contracts with third parties including Payment Gateways, Payment Processors, or Networks (as defined below).

9. Background Inquiries.

Client gives Blackbaud permission to make inquiries about Client and to obtain information about Client as may be necessary to enable Blackbaud to verify Client's identity as required from time to time by anti-money laundering laws, other applicable laws and Blackbaud's internal procedures relating to "know your client" and creditworthiness background checks. Client acknowledges that Client' business information may contain personal information about individuals related to Client and that if Client is located outside of the U.S., Blackbaud's background inquiry procedures may require such personal information be transferred into the U.S.

10. Terms Subject to Change.

The terms of this Blackbaud Payment Services Addendum (including the Exhibits attached hereto) are subject to change in Blackbaud's sole discretion. In the event of any such change, Blackbaud shall post a revision of this Addendum at http://www.blackbaud.com/files/bbms/bbpstc.pdf and Client's continued use of BBPS shall be subject to such revised terms.

Continued

blackbaud®

Appendices

EXHIBIT A, BBMS

BBMS allow you to accept payments via credit card, debit card, and ACH transactions including processing cards bearing the trademarks of Visa®, MasterCard®, Discover®, and American Express® (collectively, the "**Networks**"). Blackbaud is not a depositary institution and does not offer banking services as defined by the United States Department of Treasury. Blackbaud also does not offer Money Service Business services as defined by the United States Department of Treasury. As a merchant payment processor, Blackbaud processes payments you receive from your constituents. In order to serve in this role, we must enter into agreements with Networks, other processors, and banks. These third parties require Blackbaud's BBMS customers to enter into a Sub-Merchant Agreement with Blackbaud's payment processor of record, as set forth in Section 1 below.

1. **Sub-Merchant Agreements:** Use of BBMS requires Client's acceptance of the relevant Sub-Merchant Agreements:
   Wells Fargo Bank-Sub-Merchant Processing Agreement (https://www.blackbaud.com/files/FD-Wells_smp_agreement.pdf)
   First Data Canada-Sub-Merchant Processing Agreement (https://www.blackbaud.com/files/FD-Canada_smp_agreement.pdf)

2. **Background Checks:** Use of BBMS requires Client to provide information about Client as may be necessary to enable Blackbaud to verify Client's identity including, if applicable, verification of Client's ownership of its bank account(s) that may be used for payment purposes including deposit of processed funds as required from time to time by anti-money laundering laws, other applicable laws and Blackbaud's internal procedures relating to "know your client" and creditworthiness background checks.

3. **BBMS Processing Fees:** The processing fees applicable to BBMS ("**BBMS Processing Fees**") are located at www.blackbaud.com/bbms/bbms-tier1.aspx, as may be amended from time to time. Any changes to the BBMS Processing Fees shall take effect 30 days following the posting of any such changes. BBMS Processing Fees shall apply to all online financial transactions conducted by Client through the use of BBPS (including credit card, debit card, and ACH transactions).

4. **Disbursements:** Blackbaud will disburse to Client funds processed through BBMS, interest free, less any refunds, chargebacks, and any applicable fees (including BBMS Processing Fees and/or transaction fees related to Blackbaud Products, if applicable). Funds processed through BBMS for all Blackbaud Products other than Blackbaud Sphere shall be disbursed within five business days of the close of the following disbursement cycles: (i) the first through the seventh of each month; (ii) the eighth through the fifteenth of each month; (iii) the sixteenth through the twenty-second of each month; and (iv) the twenty-third through the end of each month. Funds processed through BBMS for Blackbaud Sphere shall be disbursed within seven business days of the close of the following disbursement cycles: (i) the first through the fifteenth of each month, and (ii) the sixteenth through the last day of each month. Blackbaud may suspend or delay disbursements to Client in order to protect Blackbaud and Client against the risk of, among other things, existing, potential or anticipated chargebacks, fraud or Client's failure to fulfill Client's responsibilities set forth in this Addendum.

5. **Client Direct Deposit ACH Form:** Client shall provide Blackbaud with a completed Authorization Agreement for Direct Deposits (ACH Credits) with Client's Taxpayer Identification Number (TIN) to permit Blackbaud to make deposits to Client's bank account in accordance with Client's disbursement instructions. Blackbaud reserves the right to hold on Client's behalf any funds collected using BBMS until Client provides such completed Authorization Agreement to Blackbaud and the verification of Client's depository bank account used in connection with BBMS.

6. **Reconciliation and Charge Backs; Debit of Client Account:** Blackbaud shall perform daily internal reconciliations and provide chargeback management services in connection with delivering statements and payment disbursements to Client. Client is responsible for its individual

transaction reconciliations for each disbursement cycle. Client is responsible for payment of all chargebacks and associated fees of any kind whatsoever against any merchant account established by Blackbaud for the purpose of consummating financial transactions conducted on behalf of Client through Blackbaud Products. For any negative transactions including refunds/chargebacks, Blackbaud reserves the right to offset such negative transactions against disbursements to Client, or if any disbursement is less than such offset, debit the Clients bank account the balance of such offset. Client agrees that Blackbaud may, without prior notice to Client, debit Client's bank account for the full amount of any negative or debit balance including chargebacks and reversals if at the end of any disbursement cycle there is a negative or debit balance in Client's BBMS account. If Blackbaud is unable to collect on Client refunds/chargebacks using offset of Client's disbursement or debit of Client's bank account, Blackbaud shall have the right to invoice Client any unpaid balance which shall be subject to the lesser of twelve percent (12%) annual interest or the highest interest allowable under applicable law.

7. **Transaction Limits:** Unless otherwise pre-approved in writing by Blackbaud, BBMS for all Blackbaud Products other than Blackbaud Sphere currently have a per transaction limit of $50,000. BBMS for Blackbaud Sphere currently have a per transaction limit of $25,000.

8. **Trust Account:** If Client is using BBMS to process transactions in U.S. dollars, Client understands and agrees that the certain Trust Account Agreement dated as of June 29, 2011 (the "**Trust Agreement**") between Blackbaud and Wells Fargo Bank, National Association (the "**Trustee**") shall govern the Trust Account that will be used for the deposit and disbursement of Client's funds processed using BBMS. Client agrees to the terms set forth in the Intended Beneficiary Disclosures located at https://www.blackbaud.com/bbms/bbms-ibd.aspx, and specifically acknowledges that Blackbaud has the right to direct payment of funds from the Trust Account created under the Trust Agreement (and the Trustee shall be entitled to rely on such direction from Blackbaud), including payments to Client and similarly situated customers of Blackbaud, the fees and expenses of Blackbaud, and certain other fees, charges, and expenses. Client specifically acknowledges and agrees that (i) the Trustee has no duty to determine whether payments requested from the Trust Account by Blackbaud are in proper amounts or for appropriate purposes, (ii) the Trustee makes no representations or warranties as to the treatment of the Trust Account in the event of any voluntary or involuntary bankruptcy, insolvency, reorganization, wind-up, or composition or adjustment of debts of Blackbaud and (iii) the Trustee cannot guarantee the timely receipt of funds by the undersigned in the event that the Trustee fails to receive directions from Blackbaud or a back-up servicer with respect to funds in the Trust Account or if there is a legal proceeding which seeks to stop or delay the disbursement of funds from the Trust Account.

9. **Reserve.**

Client acknowledges that in addition to other rights afforded to Blackbaud under the Agreement, Blackbaud, after providing reasonable prior written notice to Client, may establish a reserve account to satisfy any delinquent obligation of Client under any agreement between Client and Blackbaud (the "**Reserve Account**"). Blackbaud may (but is not required to) apply funds in the Reserve Account toward, and may set off any funds that would otherwise be payable to Client against, the satisfaction of any amounts which are or become due from Client pursuant to any such agreements. The Reserve Account will not bear interest, and Client will have no right or interest in the funds in the Reserve Account; provided that upon satisfaction of all of Client's obligations under such agreements, Blackbaud will pay to Client any funds then remaining in the Reserve Account. Any funds in the Reserve Account may be commingled with other funds, and need not be maintained in a separate account. The parties' rights and obligations under this Section shall survive the termination of the Agreement.

Continued

Exhibit A

EXHIBIT B, THIRD-PARTY MERCHANT SERVICES WITH BLACKBAUD GATEWAY INTERCONNECT OPTION

1. **Third-Party Gateway and Processor Option:** Client will be required to enter into an agreement to obtain "gateway" services directly from a Blackbaud approved third-party Payment Gateway. A list of currently approved third-party Payment Gateways can be found at www.blackbaud.com/bbms/bbms-tier3.aspx, as may be amended from time to time. Any changes to such list shall take effect 30 days following the posting of any such changes. Client further understands and agrees that Client is obligated to separately engage a Blackbaud approved third-party Payment Processor.

2. **Gateway Interconnect Fees/Rates:** The applicable Payment Gateway interconnect fees and rates ("**Interconnect Fees**") are located at www.blackbaud.com/bbms/bbms-tier3.aspx, as may be amended from time to time. Any changes to such Interconnect Fees shall take effect 30 days following the posting of any such changes.

3. **Disbursements, Reconciliation and Chargebacks:** All fund disbursements, reconciliations, and chargebacks shall be the sole responsibility of Client and the third-party Payment Gateway and third-party Payment Processor which Client has engaged. Blackbaud shall have no liability relating to any such disbursement, reconciliations, and chargebacks.

4. **Luminate Application Clients Only:** For any existing Client of Luminate Application Services who continue to use the pre-established PAYFLOW PRO gateway interface, Client acknowledges and agrees that the terms and conditions located at http://www.convio.com/Terms/Payment/Gateway/Terms/Paypal/2011/ will apply to such use. Any existing or future Client of Luminate Application Services who desires to add any additional gateway accounts must purchase such accounts directly from the third-party Payment Gateway (including PayFlow Pro gateway) and be subject to the terms and fees associated with this Addendum.

5. **onBoard and onMessage Clients Only:** Clients using onBoard or onMessage with contracts in effect on or before August 1, 2015, will have Interconnect Fees waived through the end of their contract. Interconnect Fees will begin being assessed at the time the client's contract renews. Clients using Blackbaud Merchant Services are not charged Interconnect Fees.

Continued

EXHIBIT C, BBPS SERVICE LEVELS

1. Blackbaud will install and operate BBPS at load-balanced, mirrored, highly-available, secure locations using fully-redundant equipment and networks and will monitor traffic, security, and performance on a 24x7 basis to ensure availability, capacity, security, and bandwidth.

2. Blackbaud will provide secure, encrypted access, via the Internet, to the BBPS systems from currently supported versions of Client's Blackbaud Products, from Blackbaud hosting facilities on a 24x7 basis, except for scheduled system downtime for maintenance as required and scheduled in advance by Blackbaud. Blackbaud and its vendors may perform system maintenance during the following "**BBPS Maintenance Windows**", and Blackbaud will announce all planned upgrades and outages in advance as follows:

> "**BBPS Critical Maintenance Window**" – Nightly between 10 p.m. and 12 midnight EDT/EST with at least one hour advance notice for application of critical security or software updates;
>
> "**BBPS Standard Maintenance Window**" – Sunday mornings between 3 a.m. and 7 a.m. EDT/EST, and Tuesday and Thursday between 11pm and 3am EDT/EST with at least 72 hours' advance notice; and
>
> "**BBPS Extended Maintenance Window**" – Sunday morning between 3 a.m. and 12:00 noon EDT/EST with at least 30 days' advance notice.

BBPS Maintenance Windows start and end times set forth above may be adjusted back or forward by two hours, with the same duration, upon 30 days' advance notice to Client. Blackbaud shall deliver notifications of scheduled system downtime and/or system maintenance to the Primary Contact via electronic mail. Client understands and agrees that there may be instances where Blackbaud needs to interrupt BBMS without notice in order to protect the integrity of BBMS due to security issues, virus attacks, spam issues, or other unforeseen circumstances.

3. BBPS will have a 99.9% availability rate, calculated on a monthly basis. In the event Client does not have access to its BBPS account ("**Downtime**") for more than four hours during any calendar day (other than as a result of scheduled system downtime and/or system maintenance), Client's sole and exclusive remedy and Blackbaud's sole and exclusive liability for Downtime shall be a credit to Client in an amount equal to 1/365 of the Annual Fee for Support and Maintenance paid by Client during the applicable calendar year (each such amount, a "**Credit Unit**"). Credit Units shall be reflected and applied on Client's monthly invoice for the month following the month in which a Credit Unit was credited to Client. Blackbaud will use an internal system to measure whether BBPS is available. Client agrees that Blackbaud's internal system will be the sole basis for resolution of any dispute that may arise between Client and Blackbaud regarding BBPS service levels, and further agrees not to implement or contract for any other third-party monitoring software, services, or applications for the purpose of monitoring Downtime.

4. Blackbaud will perform and retain fully restorable, data backups of encrypted BBPS databases as follows:

Backup Type	Retention	Location
Nightly	1 week	On-Site
Weekly	4 weeks	Off-Site
Monthly	6 months	Off-Site

5. Blackbaud will install minor upgrades/releases of BBPS software as they become available at no charge for the term of the Agreement. Blackbaud will determine and announce all planned upgrades as described above.

6. Customer Support hours of operation for BBPS will be provided in accordance to the Maintenance Service Plan and corresponding Scope of Support based on the subscribed level of maintenance for the Blackbaud Product using BBPS.

7. Blackbaud will monitor performance indicators on the systems and network infrastructure (its own and those of third-party vendors) in order to gauge the overall performance of BBPS, and will take reasonable steps to address systems and network infrastructure as required to maintain application performance.

8. Blackbaud will operate BBPS in accordance with PCI DSS.

Exhibit A

71C01-2112-CT-000462
St. Joseph Circuit Court
Filed: 12/15/2021 2:24 PM
Clerk
St. Joseph County, Indiana

ASPEN INSURANCE

Apex
The Pinnacle of Privacy and Network Security Insurance®

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

RAPID RESPONSE GUIDE

In consideration of the premium charged, it is agreed that,

1. The third party service providers (each a "Preferred Provider") and their respective services described in this endorsement are pre-approved by the **Insurer** to assist the **Insured** in the event of a **Privacy and Network Security Incident**. Preferred Providers are not affiliated with the **Insurer** and are solely responsible for all services.

2. **INCIDENT RESPONSE CONSULTATION HOTLINE:**

   The Incident Response Consultation Hotline (IRCH) is provided to assist the **Insured** with responding rapidly, and consistent with industry best practices, to a **Privacy and Network Security Incident**. An **Insured** calling the IRCH will be prompted to leave a voicemail, including return contact information and their Aspen Apex Policy number. The voice message will then be automatically forwarded to the **Insurer**, as well as to the **Incident Response Consultation** Preferred Provider identified in this endorsement. The **Insured** will typically receive a response from either the **Incident Response Consultation** Preferred Provider or the **Insurer** within four (4) business hours from the time such voicemail was received, however, longer response times may occur.

   Calling the IRCH is not a substitute for the **Insured's** reporting and notice obligations under the Policy. As a condition precedent to coverage, the **Insured** must comply with all obligations under the Policy, including without limitation, providing the **Insurer** notice of any incident in accordance with Section IV, Conditions B, Reporting and Notice of the Policy.

   INCIDENT RESPONSE CONSULTATION HOTLINE:

   1-844-844-0103

3. **Incident Response Consultation** Services:

   Mullen Coughlin, LLC is the exclusive Preferred Provider pre-approved by the **Insurer** to provide **Incident Response Consultation** services in connection with a **Privacy and Network Security Incident**. Any decision to engage the services of Mullen Coughlin, LLC is solely at the **Insured's** discretion.

   If the **Insured** does elect to retain the services of Mullen Coughlin, LLC, the **Insured** agrees to execute an engagement letter outlining the services to be provided. The **Insurer's** liability will only apply to **Incident Response Consultation** services provided by Mullen Coughlin, LLC, regardless of any other services that may be stated in the engagement letter between the **Insured** and Mullen Coughlin, LLC or otherwise provided by Mullen Coughlin, LLC.

4. Incident Response Services:

   Data Forensics:

   Ankura is the Preferred Provider pre-approved by the **Insurer** to provide **Data Forensics** to the **Insured** in connection with a **Privacy and Network Security Incident**. Ankura's services include:

Exhibit B

a. Evaluation and analysis of the **Insured's Network** to gather and preserve evidence for determining the breadth and source of a **Privacy and Network Security Incident**;

b. Data mining to identify the **Affected Population**; and

c. Remediation of a **Privacy and Network Security Incident** on the **Insured's Network**.

Notification, Fraud Monitoring and Resolution Services, and **Call Center Services**:

Kroll is the Preferred Provider pre-approved by the **Insurer** to provide **Notification**, **Fraud Monitoring and Resolution Services** and **Call Center Services** on behalf of the **Insured** in connection with a **Privacy and Network Security Incident**. Experian's services include:

a. Management of notification letter printing, mailing (via first class mail) and return mailing processing;

b. Change of address lookup and address verification;

c. Social Security Number verification and death registry lookup;

d. Enrollment in Triple Bureau Credit Monitoring for a period up to 12 months from the date of enrollment;

e. Enrollment in SSN Trace for individuals under the age of 18 for a period up to 12 months from the date of enrollment;

f. Automatic enrollment in Identity Monitoring, Protection, Repair and Resolution Services for a period of 12 months from the date of enrollment; and

g. **Call Center Services** for a period of up to 12 months following notification of a **Privacy and Network Security Incident**.

5. Nothing in this endorsement is meant nor will it be construed as a guarantee that the Preferred Providers will be available to provide the services described herein. The **Insurer** reserves the right to substitute a provider of like qualifications and competency in the event that a Preferred Provider is unavailable to perform the services. The **Insurer** may also change, amend or supplement its Preferred Providers from time to time for any reason. Both the **Insurer** and the **Insured** will agree in writing prior to retaining any vendor that is not a Preferred Provider.

6. Without the prior written consent of the **Insurer**, no coverage will be available under this Policy for any services performed by, or any engagement of, any third party service providers that are not specifically identified in this endorsement.

   If the **Insured** elects, with the prior written consent of the **Insurer**, to engage the services of a third party service provider not identified as a Preferred Provider in this endorsement, any **Expense** incurred will be subject to the Retention stated in Item 5 of the Declarations and will reduce the **Insurer's** maximum aggregate limit of liability stated in Item 4(B) of the Declarations upon exhaustion of the Retention.

Nothing contained herein shall be held to vary, waive, alter, or extend any of the terms, conditions, agreements or declarations of the Policy, other than as herein stated.

THIS ENDORSEMENT FORMS A PART OF POLICY NUMBER: AX008PL20

Issued by: Aspen American Insurance Company

Issued to: Trinity Health Corporation

Effective date: 07/01/2020

Exhibit B

Endorsement No.: 1

ASPEN INSURANCE

Apex
The Pinnacle of Privacy and Network Security Insurance®

NOTICE: THIS POLICY IS WRITTEN ON A CLAIMS MADE AND REPORTED BASIS. THE COVERAGE PROVIDED IS LIMITED TO ONLY THOSE CLAIMS FOR WRONGFUL ACTS TAKING PLACE ON OR AFTER THE RETROACTIVE DATE STATED IN THE DECLARATIONS AND FOR WHICH CLAIMS ARE FIRST MADE AGAINST AN INSURED DURING THE POLICY PERIOD, OR DURING ANY APPLICABLE EXTENDED REPORTING PERIOD, IF EXERCISED. INCIDENT RESPONSE EXPENSE COVERAGE APPLIES ONLY TO EXPENSE INCURRED IN CONNECTION WITH A PRIVACY AND NETWORK SECURITY INCIDENT THAT FIRST TAKES PLACE DURING THE POLICY PERIOD. PLEASE READ THE ENTIRE POLICY.

In consideration of the payment of the premium and in reliance upon the **Application**, and subject to all terms of this Policy, the **Insurer** agrees to provide coverage as follows:

I. INSURING AGREEMENTS

A. Liability and Restoration Coverage

The **Insurer** will pay, on behalf of the **Insured**, **Loss** from **Claims** first made during the **Policy Period**, and reported to the **Insurer** in accordance with the terms of this Policy, for any **Wrongful Act** which first takes place on or after the **Retroactive Date**.

B. Incident Response Expense Coverage

The **Insurer** will pay, on behalf of the **Insured**, **Expense** incurred in connection with a **Privacy and Network Security Incident** that first takes place on or after the **Retroactive Date** but prior to expiration of this Policy, and that is reported to the **Insurer** in accordance with the terms of this Policy.

II. DEFINITIONS

A. **Affected Population** means one or more individuals whose **Personal Information** was or may have been impacted as a result of a **Privacy and Network Security Incident**.

B. **Application** means any and all materials and information, submitted to the **Insurer** within the 12 months prior to the Inception Date of this Policy, in connection with a request for privacy and network security insurance coverage.

C. **Bodily Injury** means any and all physical injury, sickness, pain, suffering, disease or death of any person. **Bodily Injury** does not include mental anguish or emotional distress.

D. **Breach Notification Law** means any governmental law, statute, regulation, rule or guidance that requires notice to an **Affected Population** or governmental or regulatory authority.

E. **Call Center Services** means establishing and operating a call center in response to a **Privacy and Network Security Incident**.

F. **Claim** means any:

1. civil proceeding in a court of law or equity commenced by the filing of a complaint, motion for judgment or similar proceeding, against the **Insured**;

Exhibit B

2. written demand for monetary or non-monetary relief, written demand for arbitration or written request to toll or waive a statute of limitations received by the **Insured**;

3. administrative or regulatory proceeding, inquiry, or investigation against the **Insured**, or any regulatory response to incident reporting received by or on behalf of the **Insured**;

4. an **Extortion** event, or any other interruption to the **Insured's** ability to conduct standard business operations; or

5. deletion, destruction or manipulation of the **Insured's** data assets; or

6. loss of functionality to, destruction of, or inoperability of the **Insured's** hardware or firmware.

G. **Data Asset Restoration** means the actual, necessary and reasonable amounts paid to a third party service provider, incurred with the **Insurer's** prior written approval, to restore, or attempt to restore, the **Insured's** data assets which are compromised as a result of a **Privacy and Network Security Incident**. **Data Asset Restoration** does not include **Data Forensics** on an **Extended Network.**

H. **Data Forensics** means investigation and analysis of the **Insured's Network** to determine the source and breadth of a **Privacy and Network Security Incident.**

I. **Executive Officer** means the CEO, CFO, CISO, CIO, GC, Director of Risk Management or any individual in a functionally equivalent position of the **Insured Organization.**

J. **Expense** means the actual, necessary and reasonable amounts paid by the **Insured** to third party service providers for: **Data Forensics**, **Public Relations**, **Notification**, **Fraud Monitoring and Resolution Services**, **Call Center Services**, or **Incident Response Consultation**.

K. **Extended Network** means all desktops, laptops, servers, peripheral devices, mobile devices or other nodes not under the **Insured's** direct operational control.

L. **Extortion** means actual or threatened malicious activity directed at an **Insured's Network** or data, where payment or other action from the **Insured** is demanded by a third party.

M. **Fraud Monitoring and Resolution Services** means credit monitoring, identity monitoring, and identity restoration services provided to an **Affected Population.**

N. **Incident Response Consultation** means services provided by an external law firm to:

1. determine the applicability of and facilitate compliance with **Breach Notification Laws**;

2. draft content for **Notification** or reports to governmental or regulatory authorities; and

3. coordinate service providers approved by the **Insurer** to provide **Data Forensics**, **Public Relations**, **Data Asset Restoration, Service Restoration, Notification, Fraud Monitoring and Resolution Services**, and **Call Center Services**.

O. **Insured** means:

1. the **Insured Organization**;

2. any past, present or future director, officer, board member, trustee, owner, partner, or manager of an **Insured Organization**, but only for acts performed within the scope of their duties on behalf of the **Insured Organization**; and

3. any past, present, or future employee of an **Insured Organization**, including any full-time, part-time, temporary or leased employees, independent contractors and volunteers, but only for acts performed within the scope of their duties on behalf of the **Insured Organization**.

P. **Insured Organization** means the **Named Insured** and any **Subsidiary**. **Exhibit B**

Q. **Insurer** means the insurance company identified in the Declarations.

R. **Loss** means the following amounts for which an **Insured** becomes legally obligated to pay in connection with a **Claim**:

1. all actual, necessary and reasonable legal fees and legal expenses in the investigation, defense, or appeal of a **Claim**;
2. monetary settlements, judgements or awards, including pre-judgement and post judgement interest;
3. punitive, exemplary, or multiple damages, if and to the extent insurable by law;
4. amounts paid to a consumer redress fund;
5. fines and penalties levied by a governmental or regulatory authority, including those fines and penalties levied pursuant to the General Data Protection Regulation (GDPR) if and to the extent insurable by law, due to a **Privacy and Network Security Incident**;
6. **Data Asset Restoration** costs, regardless of any legal obligation to pay;
7. **Firmware and Hardware Asset Restoration** or **Service Restoration** costs, regardless of any legal obligation to pay; or
8. payment amounts, including the actual, reasonable and necessary costs to execute such payment, of an **Extortion** demand whether in digital currency or traditional currency, regardless of any legal obligation to pay.

Loss does not include any:

9. fines or penalties (except for those described in Section II Definitions R.5 above), assessments, sanctions or taxes;
10. future or undue profits, royalties, restitution, costs of licensing, disgorgement of profits, or unjust enrichment;
11. costs to comply with orders granting injunctive or non-monetary relief, including specific performance or any agreement to provide such relief;
12. return or offset of fees, royalties, commissions, profits or charges for goods or services already provided;
13. liquidated damages, contractually agreed penalties or similar remedies, but only to the extent such amounts exceed the amount for which the **Insured** would have been legally liable in absence of such agreement;
14. salaries, wages, fees, overhead, or any other employee benefits incurred by the **Insured**, other than those included in **Service Restoration** costs;
15. **Extortion** payment made without the prior written consent of the **Insurer**; or
16. matters which are uninsurable under applicable law.

S. **Media Incident** means any of the following, if resulting from the **Insured's** website, web-based advertising or social media activity:

1. defamation, slander, libel, trade libel, or product disparagement;
2. invasion of privacy, intrusion upon seclusion or misappropriation of likeness, picture, name, or voice;
3. intellectual property infringement;
4. plagiarism, piracy or misappropriation of ideas; or
5. domain name infringement or improper deep-linking or framing.

Exhibit B

T. **Named Insured** means the legal entity stated in Item 1 of the Declarations.

U. **Network** includes all desktops, laptops, servers, peripheral devices, mobile devices or other nodes under the **Insured's** direct operational control, whether owned or leased.

V. **Network and Information Security Controls** means all controls, whether policy or technology based, in order to prevent intrusions of or unauthorized access to, the **Network** or **Extended Network**, **Personal Information** or other data, whether residing thereon or in any other form.

W. **Notification** means communication to an **Affected Population**.

X. **Personal Information** means:

1. any non-public information that could allow an individual to be uniquely identified;

2. the definition provided in any federal, state, local or foreign privacy protection law or regulation governing the control and use of an individual's confidential or protected information; or

3. any other information associated with an individual that could be used to perpetrate identify theft or fraud.

Y. **Policy Period** means the period from the Inception Date to the Expiration Date stated in Item 2 of the Declarations.

Z. **Privacy and Network Security Incident** means any of the following:

1. an actual or suspected disclosure of **Personal Information** or the violation of a **Breach Notification Law**;

2. an actual or suspected disclosure of commercial, non-personal information due to a bypass of **Network and Information Security Controls**;

3. an actual or suspected unauthorized access to, or usage of, the **Insured's Network** due to a bypass of **Network and Information Security Controls**;

4. an **Extortion** event;

5. an inability of the **Insured** to provide products and services to customers due to a bypass of **Network and Information Security Controls**;

6. a transmission of malicious code due to a bypass of **Network and Information Security Controls**;

7. an unintentional violation of the **Insured's** own privacy policy; or

8. the misuse, mismanagement or wrongful collection of **Personal Information**

AA. **Property Damage** means physical damage to or destruction of any real or tangible property, including loss of use. For the purposes of this definition, data is not considered tangible property.

BB. **Public Relations** means services provided by an external public relations firm, crisis management firm or law firm to minimize the reputational impact on an **Insured** resulting from a **Privacy and Network Security Incident**; provided, however, that no other **Expense** or element of **Loss** will be construed as **Public Relations** services.

CC. **Related Wrongful Acts** means **Wrongful Acts** that are logically or causally connected by any common fact(s), circumstance(s), transaction(s), or event(s).

DD. **Retroactive Date** means the date stated in Item 3 of the Declarations.

EE. **Service Restoration** means the actual, necessary and reasonable amounts paid to a third party service provider or overtime pay paid to an employee of the **Insured Organization**, incurred with the **Insurer's** prior written approval, following a **Privacy and Network Security Incident**, in order to restore the operational capacity of an **Insured's Network** to the level immediately preceding such **Privacy and Network Security Incident**.

Exhibit B

FF. **Subsidiary** means any entity while the **Named Insured**:

1. owns more than 50% of its outstanding voting securities, partnership or membership interests;

2. has the right to elect or appoint a majority of such entity's directors, managers or trustees; or

3. has sole control over the management structure pursuant to a written agreement;

either directly, or indirectly through one or more **Subsidiaries**.

Any such entity that is acquired by the **Insured Organization** during the **Policy Period** and whose count of non-redundant **Personal Information** or annual revenues exceeds 25% of the **Insured Organization's**, as stated in the **Application**, will be deemed a **Subsidiary**, but only for ninety (90) days from the effective date of such acquisition.

GG. **Wrongful Act** means any actual or alleged act, error, misstatement, misleading statement, omission, neglect or breach of duty committed by an **Insured** which leads to a:

1. **Privacy and Network Security Incident**; or

2. **Media Incident**.

HH. **Firmware and Hardware Asset Restoration** means the actual, necessary and reasonable amounts, incurred with the **Insurer's** prior written approval, to purchase and replace the **Insured's** computing hardware or firmware at a replacement cost value, which are compromised as a result of a **Privacy and Network Security Incident**.

III. EXCLUSIONS

A. This Policy does not cover any **Loss**:

1. for the transfer of, or the failure to transfer, funds, monies or securities;

2. for any derivative suit or any actual or alleged violation of the Employee Retirement Income Security Act of 1974, as amended, the Securities Act of 1933, the Securities Exchange Act of 1934, or any other federal, state or local securities laws or regulations; provided however, that this Exclusion will not apply to any regulatory investigation pursuant to SEC Regulation S-P;

3. for any actual or alleged **Bodily Injury** or **Property Damage**; provided however, that this Exclusion A.3 shall not apply to **Property Damage** to computing hardware and firmware resulting from a **Privacy and Network Security Incident**;

4. based upon or arising out of any actual or alleged discharge, dispersal, release or escape of toxic chemicals, liquids or gases, waste materials or other contaminants, or pollutants, however caused;

5. based upon or arising out of any suspension or reduction in utilities or telephone communications services not under the **Insured's** control;

6. based upon or arising out of declared war by a nation state;

7. based upon or arising out of any actual or alleged infringement or misappropriation of any patent or trade secret;

8. based upon or arising out of any actual or alleged unfair competition, deceptive trade practices, restraint of trade, or antitrust;

9. based upon or arising out of employment practices;

10. based upon or arising out of any actual or alleged unsolicited communications; or

11. based upon or arising out of any actual or alleged **Claim** by any **Insured**;

Exhibit B

provided however, that Exclusions A.7. through A.11, will not apply to that portion of an otherwise covered **Claim** for a **Privacy and Network Security Incident**.

B. This Policy does not cover any **Loss** or **Expense**:

1. based upon or arising out of any actual or alleged dishonesty, fraud, criminal conduct, malicious or intentional acts or omissions by an **Insured**, or willful violation of any statute, rule or law by an **Insured**, provided, however, that this exclusion will not apply to actual, necessary and reasonable legal fees and legal expenses until there is an admission or a final, non-appealable adjudication in the underlying proceeding establishing such conduct.

   For the purpose of applying this exclusion, the conduct or knowledge of an **Insured** will not be attributed to any other **Insured** except that conduct or knowledge of an **Executive Officer** will be attributed to the **Insured Organization**.

2. based upon or arising out of:

   a. any **Claim**, **Wrongful Act**, fact, circumstance, transaction or event which has been the subject of any written notice given under any other policy before the Inception Date of this Policy;

   b. any prior or pending litigation, regulatory or administrative proceeding or any **Claim** of which the **Insured** had knowledge or received notice prior to the Inception Date of this Policy;

   c. any actual or alleged matter that prior to the Inception Date of this Policy an **Executive Officer** knew or reasonably should have known could to lead to a **Claim** or **Expense**;

   provided however, if this Policy is a renewal of an Apex privacy and network security policy issued by the **Insurer** to the **Named Insured** and continuously renewed and maintained in effect, references to the Inception Date of this Policy in Exclusions B.2.b. and B.2.c. will be deemed to refer to the inception date of the first such Apex policy.

IV. CONDITIONS

A. Limits and Retention

1. The **Insurer's** maximum aggregate limit of liability for all **Loss** covered by this Policy is stated in Item 4(A) of the Declarations.

2. The **Insurer's** maximum aggregate limit of liability for all **Notification, Fraud Monitoring and Resolution Services** and **Call Center Services** covered by this Policy is stated in Item 4(B) of the Declarations.

3. The **Insurer's** obligation to pay any **Loss** or **Expense** is in excess of the applicable Retention stated in Item 5 of the Declarations. In the event that the same or related fact(s), circumstance(s), transaction(s), or event(s) result in coverage under more than one Insuring Agreement, only the highest applicable Retention will apply. No Retention will apply to **Incident Response Consultation** or **Public Relations**.

B. Reporting and Notice

1. As a condition precedent to coverage under this Policy, the **Insured** must give the **Insurer** written notice of a **Claim** or a **Privacy and Network Security Incident** as soon as possible after such **Claim** or **Privacy and Network Security Incident** becomes known to an **Executive Officer** of the **Insured Organization**, but no later than the end of the **Policy Period** or any applicable Extended Reporting Period.

2. If, during the **Policy Period**, the **Insured** becomes aware of any **Wrongful Act** which may subsequently give rise to a **Claim** or **Privacy and Network Security Incident**, the **Insured** may give the **Insurer** written notice of such **Wrongful Act** as soon as possible after such **Wrongful Act** becomes known to an **Executive Officer** of the **Insured Organization**, but no later than the end of the **Policy Period** or any applicable Extended Reporting Period. The **Insurer** will treat any subsequently resulting **Claim** or **Privacy and Network Security Incident** as if it was first made during the **Policy Period**.

Exhibit B

3. When a **Claim** is made against the **Insured**, and there are multiple **Claims** arising from the same **Wrongful Act** or **Related Wrongful Acts**, all such **Claims** will be considered a single **Claim** and will be deemed to have been made at the time the first **Claim** was made.

C. Duty to Defend

The **Insurer** has the right and duty to defend the **Insured** in the investigation, settlement or defense of any **Claim**, even if a **Claim** is groundless, false or fraudulent. The **Insured** agrees not to make any payment, engage in any settlement negotiation, incur any **Loss**, admit liability or assume any obligation without the prior written consent of the **Insurer**.

The **Insurer** will have no obligation to pay any **Loss** or to continue to defend any **Claim** after the limit of liability stated in Item 4(A) of the Declarations has been exhausted.

D. Duty to Cooperate

The **Insured** must provide the **Insurer** with full assistance and cooperation at all times, including timely and accurate reporting and information about all incidents, **Claims**, **Loss**, and **Expense**.

E. Extended Reporting Period

1. If this Policy is cancelled or non-renewed for any reason other than non-payment of premium, the **Insured** will have an automatic Extended Reporting Period, which terminates sixty (60) days after the end of the **Policy Period**.

2. If this Policy is cancelled or non-renewed for any reason other than non-payment of premium, the **Named Insured** also has the right, within sixty (60) days of the end of the **Policy Period**, to purchase an additional Extended Reporting Period for additional premium, as stated in Item 7 of the Declarations. Once purchased, the premium for the Extended Reporting Period will be deemed fully earned.

3. If the additional Extended Reporting Period is purchased, the additional premium and effective dates will be stated in the Extended Reporting Period endorsement.

4. The Extended Reporting Period does not increase or reinstate the **Insurer's** limits of liability stated in the Declarations and this Policy does not cover **Loss** or **Expense** from any **Wrongful Act** which first takes place after the end of the **Policy Period**.

F. Other Insurance

Any coverage provided under this Policy will be primary with respect to **Privacy and Network Security Incidents**, but shall be excess over and will not contribute with any other valid and collectible insurance providing any other coverage that may be afforded under this Policy, including without limitation media liability, professional liability or any other coverage, unless such other insurance is specifically written as excess over this Policy.

G. Change In Control

If the **Named Insured** merges with or is acquired by another organization or a receiver, conservator, trustee, liquidator or rehabilitator is appointed to take control of, supervise, manage or liquidate the **Named Insured**, coverage under this Policy will continue until the end of the **Policy Period**, but only with respect to **Wrongful Acts** which first took place prior to the effective date of such merger, acquisition or appointment. The premium for this Policy will be deemed fully earned as of the effective date of such merger, acquisition or appointment.

H. Subrogation

If any payment is made under this Policy for **Loss** or **Expense**, and there is the ability to recover against any third party, it is agreed that the **Insured** tenders all its rights of recovery to the **Insurer**. The **Insured** also agrees to assist the **Insurer** in exercising such rights. Any recovery will first be paid to the **Insurer** toward any incurred subrogation expenses, **Loss** or **Expense**, and any remaining amounts will be paid to the **Insured** for reimbursement of any Retention paid.

I. Representations

Exhibit B

The **Insured** agrees that all representations made and statements contained within the **Application** for this Policy are true, accurate, and complete. Such statements and information are the basis for the **Insurer's** issuance of this Policy and are incorporated into and constitute a part of this Policy. In the event of any material untruth, inaccurate or incomplete information or misrepresentation in the **Application**, this Policy will be void ab initio if an **Executive Officer** knew as of the date of the **Application** the facts that were untrue, inaccurate, incomplete or misrepresented.

J. Cancellation

The **Insurer** may not cancel this Policy except for failure to pay premium when due, in which event, the **Insurer** will provide written notice of cancellation to the **Named Insured** at the address stated in Item 1 of the Declarations. Such notice will be mailed to the **Named Insured** at least 10 days prior to the effective cancellation date, and a copy will be sent to the **Named Insured's** agent of record.

This Policy may be cancelled by the **Named Insured** by providing written notice to the **Insurer** stating the effective date of cancellation. The **Insurer** shall return the unearned pro rata proportion of the premium as of the effective date of cancellation.

K. Alternative Dispute Resolution

If a dispute arises between **Insured** and **Insurer** in connection with this Policy and cannot be resolved through informal negotiation, the parties will attempt to resolve the dispute through mediation before a mutually agreeable mediator. The mediator's expenses and fees will be split equally by the parties. If the dispute has not been resolved upon conclusion of the mediation process, then either party may file suit in any court having jurisdiction over the parties and the subject matter of the dispute or disagreement.

L. Legal Representatives, Spouses and Domestic Partners

The legal representatives, estate, heirs, spouse or any domestic partner of an **Insured** person will be considered an **Insured** under this Policy, but only for **Claims** against such person arising solely from their status as such, and, with respect to a spouse or domestic partner, only where such **Claim** seeks amounts from marital or jointly owned property or property transferred from an **Insured** to such spouse or domestic partner.

M. Coverage Territory

The coverage under this Policy applies anywhere in the world.

N. Authorization and Notices

The **Named Insured** will act on behalf of all **Insureds** with respect to providing and receiving notices of cancellation or nonrenewal, paying premiums, receiving any return premium or electing to purchase any Extended Reporting Period.

O. Entire Agreement

The **Insured** agrees that this Policy, including the **Application** and any endorsements, constitutes the entire agreement between the **Insured** and the **Insurer** relating to this insurance. The terms, conditions and limitations of this Policy can only be waived or changed by written endorsement issued by the **Insurer**.

P. Assignment

No assignment of interest under this Policy will bind the **Insurer** without its written consent.

Q. Headings

The descriptions in the headings of this Policy are only intended for convenience and are not part of the Policy.

Exhibit B

Aspen American Insurance Company

ASPEN

IN WITNESS WHEREOF, the Insurer has caused this Policy to be signed by its President and Secretary and countersigned where required by law on the Declarations page by its duly Authorized Representative.

Secretary

President

Exhibit B

Aspen American Insurance Company

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

OFAC ENDORSEMENT

In consideration of the premium charged, it is agreed that any payment under this Policy shall only be made in full compliance with all U.S.A economic or trade sanctions or other laws or regulations, including sanctions, laws and regulations administered and enforced by the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC").

ALL OTHER TERMS, CONDITIONS AND EXCLUSIONS REMAIN UNCHANGED.

ASPEN INSURANCE

Apex
The Pinnacle of Privacy and Network Security Insurance

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

ADDITIONAL INSURED ENDORSEMENT

In consideration of the premium charged, it is agreed that the definition of **Insured** as stated in Section II, Definitions O. of this Policy is amended to include any person or entity that the **Insured Organization** has agreed to indemnify pursuant to a written contract or agreement, but only for any **Wrongful Act** by the **Insured Organization**.

Nothing contained herein shall be held to vary, waive, alter, or extend any of the terms, conditions, agreements or declarations of the Policy, other than as herein stated.

THIS ENDORSEMENT FORMS A PART OF POLICY NUMBER: AX008PL20

Issued by: Aspen American Insurance Company

Issued to: Trinity Health Corporation

Effective date: 07/01/2020

Exhibit B

Endorsement No.: 2

ASPEN INSURANCE

Apex
The Pinnacle of Privacy and Network Security Insurance

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

AGGREGATE LIMIT ENDORSEMENT

In consideration of the premium charged, it is agreed that:

1. Item 4 of the Declarations is amended to read in its entirety as follows:

   ITEM 4. LIMITS: Aggregate Limit: [redacted]

2. Section IV, Conditions, A. Limits and Retention, of this Policy is amended to read in its entirety as follows:

   1. The **Insurer's** maximum aggregate limit of liability for all **Loss** and **Expense** covered by this Policy is stated in Item 4 of the Declarations.

   2. The **Insurer's** obligation to pay any **Loss** or **Expense** is in excess of the applicable Retention set forth in Item 5 of the Declarations. In the event that the same or related fact(s), circumstance(s), transaction(s), or event(s) result in coverage under more than one Insuring Agreement, only the highest applicable Retention will apply. No Retention will apply to **Incident Response Consultation** or **Public Relations**.

Nothing contained herein shall be held to vary, waive, alter, or extend any of the terms, conditions, agreements or declarations of the Policy, other than as herein stated.

THIS ENDORSEMENT FORMS A PART OF POLICY NUMBER: AX008PL20

Issued by: Aspen American Insurance Company

Issued to: Trinity Health Corporation

Effective date: 07/01/2020

Exhibit B

Endorsement No.: 3

ASPEN INSURANCE

Apex
The Pinnacle of Privacy and Network Security Insurance

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

BORDEREAU REPORTING ENDORSEMENT

In consideration of the premium charged, it is agreed that subparagraphs 1 and 2 of Section IV, Conditions B, Reporting and Notice, of this Policy are amended to read in their entirety as follows:

1. As a condition precedent to coverage under this Policy, the **Insured** must give the **Insurer** written notice of a **Claim** or a **Privacy and Network Security Incident** as soon as possible after such **Claim** or **Privacy and Network Security Incident** becomes known to an **Executive Officer** of the **Insured Organization** if the **Insured** reasonably expects that **Loss** and **Expense** incurred in connection with such **Claim** or **Privacy and Network Security Incident** will exceed 25% of the Retention set forth in Item 5 of the Declarations. The **Insured** must provide the **Insurer** with a quarterly bordereau report of all **Claims** and **Privacy and Network Security Incidents** known to an **Executive Officer** of the **Insured Organization**, with the first bordereau report due 60 days after the Inception Date of this Policy.

   Regardless of the expected **Loss** or **Expense** associated with any **Claim** or **Privacy and Network Security Incident**, as a condition precedent to coverage under this Policy, all such **Claims** and **Privacy and Network Security Incidents** must be reported to the **Insurer** in writing no later than the end of the **Policy Period** or any applicable Extended Reporting Period.

2. If, during the **Policy Period**, the **Insured** becomes aware of any **Wrongful Act** which may subsequently give rise to a **Claim**, the **Insured** will give the **Insurer** written notice of such **Wrongful Act** as soon as possible after such **Wrongful Act** becomes known to an **Executive Officer** of the **Insured Organization** if the **Insured** reasonably expects that **Loss** on account of such **Claim** will exceed 25% of the Retention set forth in Item 5 of the Declarations. The **Insured** must provide the **Insurer** with a quarterly bordereau report of all **Wrongful Acts** known to an **Executive Officer** of the **Insured Organization**, with the first bordereau report due 60 days after the Inception Date of this Policy.

   If the **Insurer** receives written notice of a **Wrongful Act** no later than the end of the **Policy Period** or any applicable Extended Reporting Period, the **Insurer** will treat any subsequently resulting **Claim** as if it was first made during the **Policy Period**.

Nothing contained herein shall be held to vary, waive, alter, or extend any of the terms, conditions, agreements or declarations of the Policy, other than as herein stated.

THIS ENDORSEMENT FORMS A PART OF POLICY NUMBER: AX008PL20

Issued by: Aspen American Insurance Company

Issued to: Trinity Health Corporation

Effective date: 07/01/2020

Endorsement No.: 4

Exhibit B

ASPEN INSURANCE

Apex
The Pinnacle of Privacy and Network Security Insurance

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

OFFLINE MEDIA COVERAGE ENDORSEMENT

In consideration of the premium charged, it is agreed that the definition of **Media Incident** as stated in Section II, Definitions S. of this Policy is amended to read in its entirety as follows:

S. **Media Incident** means any of the following if resulting from the **Insured's** online or offline activities:

1. defamation, slander, libel, trade libel, or product disparagement;
2. invasion of privacy, intrusion upon seclusion or misappropriation of likeness, picture, name, or voice;
3. intellectual property infringement;
4. plagiarism, piracy or misappropriation of ideas; or
5. domain name infringement or improper deep-linking or framing.

Nothing contained herein shall be held to vary, waive, alter, or extend any of the terms, conditions, agreements or declarations of the Policy, other than as herein stated.

THIS ENDORSEMENT FORMS A PART OF POLICY NUMBER: AX008PL20

Issued by: Aspen American Insurance Company

Issued to: Trinity Health Corporation

Effective date: 07/01/2020

Endorsement No.: 5

Exhibit B

ASPEN INSURANCE

Apex
The Pinnacle of Privacy and Network Security Insurance

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

PAYMENT CARD COVERAGE ENDORSEMENT

In consideration of the premium charged, it is agreed that:

1. The **Insurer** will reimburse the **Insured** for:

   a. fines, penalties or assessments imposed against an **Insured** for failure to comply with any requirement of the Payment Card Industry Data Security Standards ("**PCI-DSS Fines**") due to a **Privacy and Network Security Incident** that first takes place on or after the **Retroactive Date** but prior to expiration of this Policy; and

   b. the actual, necessary and reasonable amounts incurred by an **Insured** to hire a Payment Card Industry Forensic Investigator to investigate, analyze and determine the source and breadth of a **Privacy and Network Security Incident** affecting the **Insured's** payment card systems ("**PFI Costs**") that first takes place on or after the **Retroactive Date** but prior to expiration of this Policy.

2. The **Insurer's** maximum aggregate limit of liability for all **PCI-DSS Fines** and all **PFI Costs** will be [redacted] which amount is part of and not in addition to the **Insurer's** maximum aggregate limit of liability stated in Item 4(A) of the Declarations.

Nothing contained herein shall be held to vary, waive, alter, or extend any of the terms, conditions, agreements or declarations of the Policy, other than as herein stated.

THIS ENDORSEMENT FORMS A PART OF POLICY NUMBER: AX008PL20

Issued by: Aspen American Insurance Company

Issued to: Trinity Health Corporation

Effective date: 07/01/2020

Endorsement No.: 6

ASPEN INSURANCE

Apex
The Pinnacle of Privacy and Network Security Insurance

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

PROFESSIONAL SERVICES COVERAGE ENDORSEMENT

In consideration of the premium charged, it is agreed that:

1. Section **I. Insuring Agreements**, of this Policy is amended to include the following:

   Disciplinary Proceedings Coverage

   The **Insurer** will reimburse the **Insured** for all **Loss** from **Disciplinary Proceedings** first commenced against the **Insured** and reported to the **Insurer** during the **Policy Period**.

2. The definition of **Loss**, as stated in Section **II. Definitions, R.** of this Policy is amended to include amounts an **Insured** becomes legally obligated to pay in connection with a **Disciplinary Proceeding**; provided, however, **Loss** does not include any costs or expenses incurred to correct, re-perform, or complete any **Professional Services**, except for those costs reasonably expected to mitigate or settle a **Claim** but only if **Insurer** consents in writing prior to the **Insured** incurring such costs.

3. The definition of **Wrongful Act**, as stated in Section **II. Definitions, GG.** of this Policy is amended to include any actual or alleged act, error, misstatement, misleading statement, omission, neglect or breach of duty committed by an **Insured** which leads to a **Professional Services Incident**.

4. Section **II. Definitions** of this Policy is amended to include the following terms:

   a. **Disciplinary Proceeding** means any proceeding commenced by a regulatory, disciplinary or licensing body with authority to regulate or oversee the conduct of **Professional Services** to investigate actual or alleged professional misconduct of the **Insured**.

   b. **Professional Services** means provided to others for a fee or other consideration.

   c. **Professional Services Incident** means the failure in rendering, or the failure to render **Professional Services.**

5. No coverage will be available under **I. INSURING AGREEMENTS A. Liability and Restoration Coverage**, of this Policy for any **Loss** resulting from any **Disciplinary Proceeding.**

6. No coverage will be available under this Policy for **Loss**:

   a. based upon or arising out of any actual or alleged insurance agent or brokerage advice or services; real estate agent or brokerage advice or services; financial or investment advice or services; attestation of financial statements; advice or services in connection with mergers, acquisitions, or security offerings; business valuation advice or services; legal or actuarial advice or services; engineering, architectural or design advice or services; appraising and inspecting advice or services; or medical advice or services; provided, however, that this Exclusion shall not apply to that portion of an otherwise covered Claim for a Privacy and Network Security Incident;

Exhibit B

b. based upon or arising out of any actual or alleged manufacturing of hardware products; provided, however, that this Exclusion shall not apply to that portion of an otherwise covered **Claim** for a **Privacy and Network Security Incident**;

c. based upon or arising out of any actual or alleged inaccurate, inadequate or incomplete description in the price of goods, products, services, estimates or fees; or

d. based upon or arising out of any actual or alleged sexual abuse or molestation.

7. The **Insurer's** maximum aggregate limit of liability for all **Loss** from all **Disciplinary Proceedings** is [redacted], which amount is in addition to, and not part of, the **Insurer's** maximum aggregate limit of liability stated in Item 4(A) of the Declarations. No Retention will apply to **Loss** from any **Disciplinary Proceeding**

8. The **Insurer's** maximum aggregate limit of liability for all **Loss** from **Professional Services Incidents** is [redacted], which amount is part of and not in addition to the **Insurer's** maximum aggregate limit of liability stated in Item 4(A) of the Declarations.

9. Solely with respect to **Claims** for **Professional Services Incidents**, Item 5 of the Declarations is amended to read in its entirety as follows: Item 5. Retention: [redacted]

10. Solely with respect to the coverage provided under this Endorsement which is subject to a **Retroactive Date**, Item 3. of the Declarations is deemed amended to reflect that the following **Retroactive Date** shall apply: 1/1/2010.

Nothing contained herein shall be held to vary, waive, alter, or extend any of the terms, conditions, agreements or declarations of the Policy, other than as herein stated.

THIS ENDORSEMENT FORMS A PART OF POLICY NUMBER: AX008PL20

Issued by: Aspen American Insurance Company

Issued to: Trinity Health Corporation

Effective date: 07/01/2020

Exhibit B

Endorsement No.: 7

ASPEN INSURANCE

Apex
The Pinnacle of Privacy and Network Security Insurance

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

REPUTATIONAL HARM LOST INCOME ENDORSEMENT

In consideration of the premium charged, it is agreed that:

1. Section II, Definitions is amended to include the following:

   Reputational Harm means an adverse media publication or report by a third party about the **Insured Organization** arising out of a **Privacy and Network Security Incident**.

   Reputational Harm Lost Income means the difference in net profit, before taxes, between what the **Insured Organization** earned during the 90 days following a **Reputational Harm** event and what it potentially would have earned for the same time period if the **Reputation Harm** event had not occurred.

2. Section II, Definition F. **Claim** is amended to include **Reputational Harm**.

3. Section II, Definition R. **Loss** is amended to include **Reputational Harm Income Loss.**

4. The **Insurer's** maximum aggregate limit of liability for all **Reputational Harm Income Loss** will be [redacted], which amount is part of and not in addition to the **Insurer's** maximum aggregate limit of liability stated in Item 4(A) of the Declarations

5. The amount of **Reputational Harm Income Loss** will be calculated by an independent third party forensic accountant, to be mutually agreed upon in writing by the **Insurer** and the **Insured**, taking into account both the **Insured Organization's** net profit or loss during the 12 month period immediately preceding the **Reputational Harm** that gave rise to the **Reputational Harm Income Loss** and the net profit or loss the **Insured Organization** potentially could have generated had the **Reputational Harm** not occurred.

6. Solely with respect to **Reputational Harm**, Item 5 of the Declarations is amended to read in its entirety as follows:

   Item 5. Retention: [redacted]

Nothing contained herein shall be held to vary, waive, alter, or extend any of the terms, conditions, agreements or declarations of the Policy, other than as herein stated.

THIS ENDORSEMENT FORMS A PART OF POLICY NUMBER: AX008PL20

Issued by: Aspen American Insurance Company

Issued to: Trinity Health Corporation

Effective date: 07/01/2020

Exhibit B

Endorsement No.: 8

ASPEN INSURANCE

Apex
The Pinnacle of Privacy and Network Security Insurance

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

TELECOMMUNICATIONS FRAUD ENDORSEMENT

In consideration of the premium charged, it is agreed that:

1. Section II, Definitions is amended to include the following:

   Telecommunications Fraud means any unauthorized access to or use of the **Insured Organization's** telephone system by a third party which results in **Telecommunications Fraud Loss.**

   Telecommunications Fraud Loss means any charges incurred by the **Insured Organization** resulting directly from **Telecommunications Fraud**, not including any amounts reversed by the **Insured Organization's** telecommunications provider.

2. Section II, Definition F. **Claim** is amended to include **Telecommunications Fraud**.

3. Section II, Definition R. **Loss** is amended to include **Telecommunications Fraud Loss.**

4. The **Insurer's** maximum aggregate limit of liability for all **Telecommunications Fraud Loss** will be [redacted], which amount is part of and not in addition to the **Insurer's** maximum aggregate limit of liability stated in Item 4(A) of the Declarations

5. Solely with respect to **Telecommunications Fraud**, Item 5 of the Declarations is amended to read in its entirety as follows:

   Item 5. Retention: [redacted]

Nothing contained herein shall be held to vary, waive, alter, or extend any of the terms, conditions, agreements or declarations of the Policy, other than as herein stated.

THIS ENDORSEMENT FORMS A PART OF POLICY NUMBER: AX008PL20

Issued by: Aspen American Insurance Company

Issued to: Trinity Health Corporation

Effective date: 07/01/2020

Exhibit B

Endorsement No.: 9

ASPEN INSURANCE

Apex
The Pinnacle of Privacy and Network Security Insurance

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

AMEND DEFINITION OF DATA ASSET RESTORATION ENDORSEMENT

In consideration of the premium charged, it is agreed that Section II, Definitions G. of this Policy is amended to read in its entirety as follows:

G. **Data Asset Restoration** means the actual, necessary and reasonable amounts paid to a third party service provider, incurred with the **Insurer's** prior written approval, to restore, or attempt to restore, the **Insured's** data assets which are compromised as a result of bricking or a **Privacy and Network Security Incident**.

Nothing contained herein shall be held to vary, waive, alter, or extend any of the terms, conditions, agreements or declarations of the Policy, other than as herein stated.

THIS ENDORSEMENT FORMS A PART OF POLICY NUMBER: AX008PL20

Issued by: Aspen American Insurance Company

Issued to: Trinity Health Corporation

Effective date: 07/01/2020

Endorsement No.: 10

Exhibit B

ASPEN INSURANCE

Apex
The Pinnacle of Privacy and Network Security Insurance

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

AMEND DEFINITION OF EXTORTION AND LOSS ENDORSEMENT

In consideration of the premium charged, it is agreed that:

1. Section II, Definitions L. of this Policy is amended to read in its entirety as follows:

   L. **Extortion** means actual or threatened malicious activity, including ransomware, directed at:

      1. an **Insured's Network** or data; or

      2. any customer of the **Insured** through access to the **Insured's Network**;

      where payment or other action from the **Insured** is demanded by a third party.

2. Section II, Definitions R.15. of this Policy is amended to read in its entirety as follows:

   15. **Extortion** payment made without the prior written consent of the **Insurer**; provided that the **Insurer** agrees that the **Insured** may make an **Extortion** payment without prior written consent of the **Insurer** wherein such payment does not exceed twenty-five percent (25%) of Retention stated in Item 5 of the Declarations.

Nothing contained herein shall be held to vary, waive, alter, or extend any of the terms, conditions, agreements or declarations of the Policy, other than as herein stated.

THIS ENDORSEMENT FORMS A PART OF POLICY NUMBER: AX008PL20

Issued by: Aspen American Insurance Company

Issued to: Trinity Health Corporation

Effective date: 07/01/2020

Endorsement No.: 11

Exhibit B

ASPEN INSURANCE

Apex
The Pinnacle of Privacy and Network Security Insurance

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

AMEND DEFINITION OF SUBSIDIARY ENDORSEMENT

In consideration of the premium charged, it is agreed that the definition of **Subsidiary** as stated in Section II, Definitions FF. of this Policy is amended to read in its entirety as follows:

FF. Subsidiary means any entity while the **Named Insured**:

1. owns more than 50% of its outstanding voting securities, partnership or membership interests;
2. has the right to elect or appoint a majority of such entity's directors, managers or trustees; or
3. has sole control over the management structure pursuant to a written agreement;

either directly, or indirectly through one or more **Subsidiaries**.

Any such entity that is acquired by the **Insured Organization** during the **Policy Period** and whose annual revenues exceeds 25% of the **Insured Organization's**, as stated in the **Application**, will be deemed a **Subsidiary**, but only for ninety (90) days from the effective date of such acquisition.

Any such entity that is acquired by the **Insured Organization** during the **Policy Period** and whose annual revenues is equal to or less than 25% of the **Insured Organization's**, as stated in the **Application**, will be automatically deemed a **Subsidiary**.

Nothing contained herein shall be held to vary, waive, alter, or extend any of the terms, conditions, agreements or declarations of the Policy, other than as herein stated.

THIS ENDORSEMENT FORMS A PART OF POLICY NUMBER: AX008PL20

Issued by: Aspen American Insurance Company

Issued to: Trinity Health Corporation

Effective date: 07/01/2020

Endorsement No.: 12

Exhibit B

ASPEN INSURANCE

Apex
The Pinnacle of Privacy and Network Security Insurance

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

AMEND LIMITS APPLICABLE TO DATA FORENSICS AND PRE-APPROVED VENDOR WITH RATES ENDORSEMENT

In consideration of the premium charged, it is agreed that:

1. **ITEM 4. LIMITS** of the Declarations for this Policy is amended to include the following:

   (C) Aggregate Limit C: [redacted]

2. Section **IV. CONDITIONS**, Paragraph **A.**, Limits and Retention, is amended to include the following:

   The **Insurer's** maximum aggregate limit of liability for all **Data Forensics** covered by this Policy is stated in Item 4(C) of the Declarations, which shall be part of and not in addition to the limit of liability stated in Item 4(A) of the Declarations.

3. Notwithstanding Paragraph **4.** of the Rapid Response Guide and subject to the limit of liability stated in Item 4(C) of the Declarations, the below vendors are approved to provide **Data Forensics** to the **Insured** in connection with a **Privacy and Network Security Incident** covered by this Policy. The **Insurer** will pay such vendors, on behalf of the **Insured**, in accordance with the hourly rates set forth below. Any amounts charged by such vendors or otherwise incurred in excess of the hourly rates set forth below will be borne by the **Insured** uninsured and at its own risk:

Vendors	Hourly Rates
Mandiant, PwC, Optiv, KPMG, Dell Secureworks, Ernst & Young	[redacted] per hour

Nothing contained herein shall be held to vary, waive, alter, or extend any of the terms, conditions, agreements or declarations of the Policy, other than as herein stated.

THIS ENDORSEMENT FORMS A PART OF POLICY NUMBER: AX008PL20

Issued by: Aspen American Insurance Company

Issued to: Trinity Health Corporation

Effective date: 07/01/2020

Endorsement No.: 13

Exhibit B

ASPEN INSURANCE

Apex
The Pinnacle of Privacy and Network Security Insurance

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

VOLUNTARY TAKEDOWN ENDORSEMENT

In consideration of the premium charged, it is agreed that:

1. The definition of **Privacy and Network Security Incident**, as stated in Section II, Definitions Z., of this Policy is amended to include:

   9. an inability of the **Insured** to provide products and services to customers due to a voluntary takedown of the **Insured's Network** to avoid, minimize or thwart a bypass of **Network and Information Security Controls.**

2. The **Insurer's** maximum aggregate limit of liability for all **Service Restoration** from a voluntary takedown affecting the **Insured's Network** will be [redacted], which amount is part of and not in addition to the **Insurer's** maximum aggregate limit of liability stated in Item 4(A) of the Declarations.

3. The **Insurer's** maximum aggregate limit of liability for all **Business Income Loss** from a voluntary takedown affecting the **Insured's Network** will be [redacted], which amount is part of and not in addition to the **Insurer's** maximum aggregate limit of liability stated in Item 4(A) of the Declarations.

4. The amount of **Business Income Loss** will be calculated by an independent third party forensic accountant, to be agreed mutually agreed upon in writing by the **Insurer** and the **Insured**, taking into account both the **Insured Organization's** net profit or loss during the 90 day period immediately preceding the voluntary takedown that gave rise to the **Business Income Loss** and the net profit or loss the **Insured Organization** potentially could have generated had the voluntary takedown not occurred.

5. For the purposes of the coverage granted pursuant to this endorsement, **Business Income Loss** shall have the meaning set forth in Endorsement 15.

Nothing contained herein shall be held to vary, waive, alter, or extend any of the terms, conditions, agreements or declarations of the Policy, other than as herein stated.

THIS ENDORSEMENT FORMS A PART OF POLICY NUMBER: AX008PL20

Issued by: Aspen American Insurance Company

Issued to: Trinity Health Corporation

Effective date: 07/01/2020

Exhibit B

Endorsement No.: 14

ASPEN INSURANCE

Apex
The Pinnacle of Privacy and Network Security Insurance

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

BUSINESS INCOME LOSS (INCLUDING CONTINGENT) COVERAGE ENDORSEMENT

In consideration of the premium charged, it is agreed that:

1. Solely with respect to **Claims** for **Business Income Loss**, Item 5 of the Declarations is amended to read in its entirety as follows:

   Item 5. Retention: [redacted] for each event affecting the **Insured's Network**
   [redacted] for each event affecting an **Extended Network**

2. Section II, Definitions, of this Policy is amended to include the following term:

   Business Income Loss means the net profit, before taxes, that the **Insured Organization** would have earned during a period of disruption to:

   1. the **Insured's** business operations due to a **Privacy and Network Security Incident**, or

   2. an **Extended Network** due to an event affecting such **Extended Network** that would have constituted a Privacy and Network Security Incident if it had occurred on the **Insured's Network**.

3. The definition of **Loss**, as stated in Section II, Definitions R., of this Policy is amended to include **Business Income Loss**.

4. The Insurer's maximum aggregate limit of liability for all Business Income Loss from all events affecting the Insured's Network will be [redacted], which amount is part of and not in addition to the Insurer's maximum aggregate limit of liability stated in Item 4(A) of the Declarations. The Insurer's maximum aggregate limit of liability for all Business Income Loss from all events affecting all Extended Networks will be [redacted], with [redacted] affecting all Extended Networks and [redacted] affecting an Extended Network maintained by Cerner Corporation, Microsoft Corp, McKesson Technology Solutions, Cisco, Change Healthcare, 3M Health Information Systems, AT&T, Tierpoint New York LLC, Epic Systems Corporation, Oracle America Inc, Infor Us Inc, Workday Inc, ADP, IBM Corp, Informatica Corporation, Medical Information Technology (Meditech), White Harris, Careevolution Inc, Verizon Wireless, Kronos Incorporated, Centurylink, Allscripts, Nextgen Healthcare Practice, Homecare Homebase LLC, Teradata Operations Inc, Level 3 Communications LLC, Time Warner Cable, Nuance Communications, Athenahealth, PNC, General Electric, Amerisource Bergenwhich amount is part of and not in addition to the Insurer's maximum aggregate limit of liability stated in Item 4(A) of the Declarations. Business Income Loss affecting all Extended Networks is covered for up to 120 days upon contract execution.

Exhibit B

5. The amount of **Business Income Loss** will be calculated by an independent third party forensic accountant, to be agreed mutually agreed upon in writing by the **Insurer** and the **Insured**, and paid for by the **Insurer**, taking into account both the **Insured Organization's** net profit or loss during the 90 day period immediately preceding the **Privacy and Network Security Incident** or event affecting the **Extended Network** that gave rise to the **Business Income Loss** and the net profit or loss the **Insured Organization** potentially could have generated had the **Privacy and Network Security Incident** or event affecting the **Extended Network** not occurred.

Nothing contained herein shall be held to vary, waive, alter, or extend any of the terms, conditions, agreements or declarations of the Policy, other than as herein stated.

THIS ENDORSEMENT FORMS A PART OF POLICY NUMBER: AX008PL20

Issued by: Aspen American Insurance Company

Issued to: Trinity Health Corporation

Effective date: 07/01/2020

Exhibit B

Endorsement No.: 15

ASPEN INSURANCE

Apex
The Pinnacle of Privacy and Network Security Insurance

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

TRANSFER OF FUNDS AND FRAUDULENT INSTRUCTION COVERAGE ENDORSEMENT

In consideration of the premium charged, it is agreed that:

1. The definition of **Loss**, as stated in Section II, Definitions R, of this Policy is amended to include the transfer or loss of funds, monies or securities due to a **Privacy and Network Security Incident** or a **Fraudulent Instruction Incident**.

2. The definition of **Claim**, as stated in Section II, Definitions F.4. of this Policy is amended to include a **Fraudulent Instruction Incident**.

3. Section II, Definitions is amended to include the following:

   Fraudulent Instruction Incident means:

   1. the intentional misleading of and/or misrepresentation of facts to an **Insured,** committed by a third party purporting to be a vendor, business associate, client, or an employee of the **Insured**, which results in the **Insured's** transfer of funds, monies or securities; or

   2. the intentional misleading of and/or misrepresentation of facts by a third party purporting to be an **Insured** following a **Privacy and Network Security Incident** on the **Insured's Network**, to a vendor, business associate or client of the **Insured**, which results in the transfer of funds, monies or securities.

4. Section III, Exclusions A.1. of this Policy is amended to read in its entirety as follows:

   1. for the failure to transfer funds, monies or securities;

5. Section III. Exclusion A.1. of this Policy is amended to include the following:

   a. transfer of funds, monies or securities by any **Insured** for personal gain, whether acting alone or in collusion with others

6. Section IV. Conditions B.1. of this Policy is amended to read in its entirety as follows:

   1. As a condition precedent to coverage under this Policy, the **Insured** must give the **Insurer** written notice of a **Claim**, **Privacy and Network Security Incident** or **Fraudulent Instruction Incident** as soon as possible after such **Claim**, **Privacy and Network Security Incident** or **Fraudulent Instruction Incident** becomes known to an **Executive Officer** of the **Insured Organization**, but no later than the end of the **Policy Period** or any applicable Extended Reporting Period.

7. The **Insurer's** maximum aggregate limit of liability for the transfer or loss of funds, monies or securities due to a **Fraudulent Instruction Incident** will be [redacted], which amount is part of and not in addition to the **Insurer's** maximum aggregate limit of liability stated in Item 4(A) of the Declarations.

Exhibit B

8. Solely with respect to the transfer or loss of funds, monies or securities due to a **Fraudulent Instruction Incident**, Item 5 of the Declarations is amended to read in its entirety as follows:

Item 5. Retention: [redacted]

Nothing contained herein shall be held to vary, waive, alter, or extend any of the terms, conditions, agreements or declarations of the Policy, other than as herein stated.

THIS ENDORSEMENT FORMS A PART OF POLICY NUMBER: AX008PL20

Issued by: Aspen American Insurance Company

Issued to: Trinity Health Corporation

Effective date: 07/01/2020

Exhibit B

Endorsement No.: 16

ASPEN INSURANCE

Apex
The Pinnacle of Privacy and Network Security Insurance

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

SYSTEM FAILURE COVERAGE ENDORSEMENT; INCLUDING DEPENDENT SYSTEM FAILURE

In consideration of the premium charged, it is agreed that:

1. Solely with respect to **Claims** for **System Failure Business Income Loss**, Item 5 of the Declarations is amended to read in its entirety as follows:

   Item 5. Retention: [redacted] for each **System Failure** of the **Insured's Network**

   [redacted] for each **System Failure** of an **Extended Network**

2. Section II, Definitions, of this Policy is amended to include the following terms:

   System Failure means an:

   a. unintentional and unplanned outage or failure of the **Insured's Network** or an **Extended Network** directly caused by a software error or glitch; or

   b. unintentional, accidental or negligent act, error or omission by the **Insured Organization** in entering or modifying data; creating, handling, developing, or maintaining data or operating or maintaining the **Insured Organization's Network**.

   System Failure Business Income Loss means the net profit, before taxes, that the **Insured Organization** would have earned during a period of disruption to the **Insured's Network** or an **Extended Network** due to a **System Failure**.

3. The definition of **Loss**, as stated in Section II, Definitions R., of this Policy is amended to include **System Failure Business Income Loss**.

4. Solely with respect to **Claims** for **System Failure Business Income Loss**, the definition of **Wrongful Act** as stated in Section II, Definitions GG. of this Policy is amended to include a **System Failure**.

5. The **Insurer's** maximum aggregate limit of liability for all **System Failure Business Income Loss** for all **System Failures** of the **Insured's Network** will be [redacted], which amount is part of and not in addition to the **Insurer's** maximum aggregate limit of liability stated in Item 4(A) of the Declarations.

6. The **Insurer's** maximum aggregate limit of liability for all **System Failure Business Income Loss** for all

Exhibit B

System Failures of an **Extended Network** will be [redacted], which amount is part of and not in addition to the **Insurer's** maximum aggregate limit of liability stated in Item 4(A) of the Declarations.

7. The amount of **System Failure Business Income Loss** will be calculated by an independent third party forensic accountant, to be mutually agreed upon in writing by the **Insurer** and the **Insured**, taking into account both the **Insured Organization's** net profit or loss during the 90 day period immediately preceding the **System Failure** that gave rise to the **System Failure Business Income Loss** and the net profit or loss the **Insured Organization** potentially could have generated had the **System Failure** not occurred.

Nothing contained herein shall be held to vary, waive, alter, or extend any of the terms, conditions, agreements or declarations of the Policy, other than as herein stated.

THIS ENDORSEMENT FORMS A PART OF POLICY NUMBER: AX008PL20

Issued by: Aspen American Insurance Company

Issued to: Trinity Health Corporation

Effective date: 07/01/2020

Endorsement No.: 17

Exhibit B

ASPEN INSURANCE

Apex
The Pinnacle of Privacy and Network Security Insurance

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

AMENDATORY ENDORSEMENT

In consideration of the premium charged, it is agreed that:

1. Section II, Definitions F. "**Claim**" of this Policy is amended to include:

   7. alternative dispute resolution proceeding.

2. Section II, Definitions G. "**Data Asset Restoration**" of this Policy is deleted in its entirety and replaced as follows:

   G. Data Asset Restoration means the necessary and reasonable amounts paid to a third party service provider, incurred with the **Insurer's** prior written approval, to restore, or attempt to restore, the **Insured's** data assets which are compromised as a result of a **Privacy and Network Security Incident. Data Asset Restoration** does not include **Data Forensics** on an **Extended Network.**

3. Section II, Definitions H. "**Data Forensics**" of this Policy is deleted in its entirety and replaced as follows:

   H. Data Forensics means investigation and analysis of the **Insured's Network** to determine the cause, source and scope of a **Privacy and Network Security Incident**.

4. Section II, Definitions I. "**Executive Officer**" of this Policy is deleted in its entirety and replaced as follows:

   I. Executive Officer means the Chief Executive Officer, Chief Information Officer, Risk Manager, General Counsel, Director of IT Security of the **Insured Organization.**

5. Section II, Definitions J. "**Expense**" of this Policy is deleted in its entirety and replaced as follows:

   J. **Expense** means the necessary and reasonable amounts paid by the **Insured** to third party service providers for: **Data Forensics, Public Relations, Notification, Fraud Monitoring and Resolution Services, Call Center Services**, or **Incident Response Consultation.**

6. Section II, Definitions K. **"Extended Network"** of this Policy is deleted in its entirety and replaced as follows:

   K. Extended Network means all desktops, laptops, servers, peripheral devices, medical and mobile devices or other nodes not under the Insured's direct operational control.

7. Section II, Definitions O. "**Insured**" of this Policy is amended by the addition of the following:

   4. Any person or organization to whom the **Named Insured** becomes obligated to include as additional **Insured** under this Policy as a result of any written contract the **Named Insured** enters into that is executed prior to any **Loss** or **Expense** which requires the **Named Insured** to furnish insurance to that person or organization of the type provided by this Policy.

Exhibit B

However, the insurance provided will not exceed the lesser of:

a. The limits of this Policy, or

b. The limits required by the written contract referenced above.

8. Section II, Definitions R.9. "**Loss**" of this Policy is deleted in its entirety and replaced as follows:

9. fines or penalties (except for those described in Section II Definitions R.5 above), assessments, sanctions or taxes imposed upon the **Insured**;

9. Section II, Definitions R.12 "**Loss**" of this Policy is deleted in its entirety and replaced as follows:

12. return or offset of fees, royalties, commissions, profits or charges for goods or services already provided; provided however, compensatory amounts equivalent to fees, royalties, commissions, profits, or charges which are used as a measure of an otherwise covered loss shall not be excluded;

10. Section II, Definitions R.14. "**Loss**" of this Policy is amended to include the following:

14. salaries, wages, fees, overhead, or any other employee benefits incurred by the **Insured**, other than those included in **Service Restoration** costs; provided however, internal costs incurred by internal IT or an internal call center;

11. Section II, Definitions S. "**Media Incident**" of this Policy is deleted in its entirety and replaced with the following:

S. **Media Incident** means any of the following, if resulting from the **Insured's** website, web-based advertising or social media activity:

1. defamation, slander, libel, trade libel, or product disparagement;

2. invasion of privacy, intrusion upon seclusion or misappropriation of likeness, picture, name, or voice;

3. intellectual property infringement;

4. plagiarism, piracy or misappropriation of ideas;

5. domain name infringement or improper deep-linking or framing;

6. false arrest, detention or imprisonment, malicious prosecution, harassment, trespass, wrongful entry or eviction, eavesdropping, false light or other invasion of the right of privacy; or

12. Section II, Definitions U. "**Network**" of this Policy is deleted in its entirety and replaced as follows:

U. **Network** includes all desktops, laptops, servers, peripheral devices, medical and mobile devices or other nodes under the **Insured's** direct operational control, whether owned or leased.

13. Section II, Definitions Z. "**Privacy and Network Security Incident**" of this Policy is deleted in its entirety and replaced with the following:

Z. **Privacy and Network Security Incident** means any of the following:

1. an actual or suspected disclosure of **Personal Information** or the violation of a **Breach Notification Law**;

2. an actual or suspected disclosure of commercial, non-personal information due to a bypass of **Network and Information Security Controls**;

Exhibit B

3. an actual or suspected unauthorized access to, or usage of, the **Insured's Network** due to a bypass of **Network and Information Security Controls**;

4. an **Extortion** event;

5. an inability of the **Insured** to provide products and services to customers due to a bypass of **Network and Information Security Controls**;

6. a transmission of malicious code due to a bypass of **Network and Information Security Controls**;

7. an unintentional violation of the **Insured's** own privacy policy;

8. the misuse, mismanagement or wrongful collection of **Personal Information**
9. loss, theft, failure to protect, or unauthorized acquisition of **Personal Information** or commercial non-personal information; or

10. violation of any law, statute or regulation governing the authenticity, availability, confidentiality, storage, control, disclosure, integrity, or use of **Personal Information**.

14. Section II, Definitions EE. "**Service Restoration**" of this Policy is deleted in its entirety and replaced as follows:

EE. Service Restoration means the necessary and reasonable amounts paid to a third party service provider or overtime pay paid to an employee of the **Insured Organization**, incurred with the **Insurer's** prior written approval, following a **Privacy and Network Security Incident**, in order to restore the operational capacity of an **Insured's Network** to the level immediately preceding such **Privacy and Network Security Incident**.

15. Section II, Definitions HH. "**Firmware and Hardware Asset Restoration**" of this Policy is deleted in its entirety and replaced as follows:

HH. Firmware and Hardware Asset Restoration means the necessary and reasonable amounts, incurred with the **Insurer's** prior written approval, to purchase and replace the **Insured's** computing hardware or firmware at a replacement cost value, which are compromised as a result of a **Privacy and Network Security Incident**.

16. Section III, Exclusions, **A.3.** of this Policy is deleted in its entirety and replaced as follows:

3. for any actual or alleged **Bodily Injury** or **Property Damage**; provided however, that this Exclusion **A.3** shall not apply to **Property Damage** to computer hardware resulting from a **Privacy and Network Security Incident;**

17. Section III, Exclusions, **B.2. a.** of this Policy is deleted in its entirety and replaced as follows:

a. any **Claim**, **Wrongful Act**, fact, circumstance, transaction or event which has been the subject of any written notice given and accepted under any other policy before the Inception Date of this Policy;

18. Section IV, Conditions, H. **Subrogation** of this Policy is deleted in its entirety and replaced as follows:

If any payment is made under this Policy for **Loss** or **Expense**, and there is the ability to recover against any third party, it is agreed that the **Insured** tenders all its rights of recovery to the **Insurer**. The **Insured** also agrees to assist the **Insurer** in exercising such rights. Any recovery will first be paid to the **Insurer** toward any incurred subrogation expenses, **Loss** or **Expense**, and any remaining amounts will be paid to the **Insured** for reimbursement of any Retention paid.

Provided however, in the event of any payment under this Policy for a **Loss** or **Expense** for which the **Insured** has waived the right of recovery in a written contract entered into prior to the **Loss** or **Expense**, the **Insurer** hereby agrees to also waive its right of recovery.

19. Section IV, Conditions E.1. and E.2. Extended Reporting Period of this Policy are deleted in their entirety and replaced as follows:

Exhibit B

1. If this Policy is cancelled or non-renewed for any reason other than non-payment of premium, the **Insured** will have an automatic Extended Reporting Period, which terminates ninety (90) days after the end of the **Policy Period**.

2. If this Policy is cancelled or non-renewed for any reason other than non-payment of premium, the **Named Insured** also has the right, within ninety (90) days of the end of the **Policy Period**, to purchase an additional Extended Reporting Period for additional premium, as stated in Item 7 of the Declarations. Once purchased, the premium for the Extended Reporting Period will be deemed fully earned.

20. The Policy is amended as follows:

1. The **Insurer** will reimburse the **Insured** for:

   a. fines, penalties or assessments imposed against an **Insured** for failure to comply with any requirement of the Payment Card Industry Data Security Standards ("**PCI-DSS Fines**") due to a **Privacy and Network Security Incident** that first takes place on or after the **Retroactive Date** but prior to expiration of this Policy; and

   b. the necessary and reasonable amounts incurred by an **Insured** to hire a Payment Card Industry Forensic Investigator to investigate, analyze and determine the source and breadth of a **Privacy and Network Security Incident** affecting the **Insured's** payment card systems ("**PFI Costs**") that first takes place on or after the **Retroactive Date** but prior to expiration of this Policy.

2. The **Insurer's** maximum aggregate limit of liability for all **PCI-DSS Fines** and all **PFI Costs** will be $«Sublimit», which amount is part of and not in addition to the **Insurer's** maximum aggregate limit of liability stated in Item 4(A) of the Declarations.

Nothing contained herein shall be held to vary, waive, alter, or extend any of the terms, conditions, agreements or declarations of the Policy, other than as herein stated.

THIS ENDORSEMENT FORMS A PART OF POLICY NUMBER: AX008PL20

Issued by: Aspen American Insurance Company

Issued to: Trinity Health Corporation

Effective date: 7/1/2020

Exhibit B

Endorsement No.: 18

POLICYHOLDER DISCLOSURE
NOTICE OF TERRORISM INSURANCE COVERAGE AND CAP ON LOSSES FROM CERTIFIED ACTS OF TERRORISM

Coverage for acts of terrorism is included in your policy. You are hereby notified that under the Terrorism Risk Insurance Act, as amended in 2015, the definition of act of terrorism has changed. As defined in Section 102(1) of the Act: The term "act of terrorism" means any act that is certified by the Secretary of the Treasury—in consultation with the Secretary of Homeland Security, and the Attorney General of the United States—to be an act of terrorism; to be a violent act or an act that is dangerous to human life, property, or infrastructure; to have resulted in damage within the United States, or outside the United States in the case of certain air carriers or vessels or the premises of a United States mission; and to have been committed by an individual or individuals as part of an effort to coerce the civilian population of the United States or to influence the policy or affect the conduct of the United States Government by coercion. Under your coverage, any losses resulting from certified acts of terrorism may be partially reimbursed by the United States Government under a formula established by the Terrorism Risk Insurance Act, as amended. However, your policy may contain other exclusions which might affect your coverage, such as an exclusion for nuclear events. Under the formula, the United States Government generally reimburses 85% through 2015; 84% beginning on January 1, 2016; 83% beginning on January 1, 2017; 82% beginning on January 1, 2018; 81% beginning on January 1, 2019 and 80% beginning on January 1, 2020 of covered terrorism losses exceeding the statutorily established deductible paid by the insurance company providing the coverage. The Terrorism Risk Insurance Act, as amended, contains a $100 billion cap that limits U.S. Government reimbursement as well as insurers' liability for losses resulting from certified acts of terrorism when the amount of such losses exceeds $100 billion in any one calendar year. If the aggregate insured losses for all insurers exceed $100 billion, your coverage may be reduced.

In accordance with the federal Terrorism Risk Insurance Act, we are required to provide you with a notice disclosing the portion of your premium, if any, attributable to coverage for terrorist acts certified under the Terrorism Risk Insurance Act. The portion of your annual premium that is attributable to coverage for acts of terrorism is $0, and does not include any charges for the portion of losses covered by the United States government under the Act.

BY RECEIPT OF THIS NOTICE YOU HAVE BEEN NOTIFIED, UNDER THE TERRORISM RISK INSURANCE ACT, AS AMENDED, THAT COVERAGE UNDER THIS POLICY FOR ANY LOSSES RESULTING FROM CERTIFIED ACTS OF TERRORISM, MAY BE PARTIALLY REIMBURSED BY THE UNITED STATES GOVERNMENT AND MAY BE SUBJECT TO A $100 BILLION CAP THAT MAY REDUCE YOUR COVERAGE. YOU HAVE ALSO BEEN NOTIFIED OF THE PORTION OF YOUR PREMIUM ATTRIBUTABLE TO SUCH COVERAGE.

Exhibit B

71C01-2112-CT-000462
St. Joseph Circuit Court
Filed: 12/15/2021 2:24 PM
Clerk
St. Joseph County, Indiana

Effective Date: June 17, 2015

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("BAA") is entered into by and between Covered Entity (as defined below) and Blackbaud, Inc. ("Business Associate") and applies to all services provided to or on behalf of the Covered Entity by Business Associate pursuant to an underlying service agreement ("Agreement").

A. Covered Entity. "Covered Entity" shall mean all affiliates of CHE-Trinity Health, individually and collectively, which have entered into a Services Agreement with Business Associate or whose affiliated foundations entered into a Services Agreement with Business Associate and are listed on Exhibit A as updated from time to time. Nothing in this Agreement shall be construed as creating a separate contractual relationship with any Covered Entity that has not entered into a Service Agreement with the Business Associate, if such a contractual relationship does not otherwise exist.

B. HIPAA and HITECH Dominance. In the event of a conflict or inconsistency between the terms of any other agreement between the parties and this language, this BAA language controls with respect to the subject matter herein. This BAA is required by the Health Insurance Portability and Accountability Act of 1996, and the Health Information Technology for Economic and Clinical Health Act (found in Title XIII of the American Recovery and Reinvestment Act of 2009) ("HIPAA" and "HITECH"). The parties acknowledge and agree that, beginning with the effective date of this BAA, Business Associate will comply with its obligations under this BAA and with all applicable obligations of a business associate under HIPAA, HITECH and any implementing regulations, as they exist at the time this BAA is executed and as they are amended from time to time, for so long as this BAA is in place. (Collectively, HIPAA and HITECH are referred to herein as "HIPAA"). The terms used in this BAA have the same meaning as defined by HIPAA unless the context dictates otherwise.

C. HIPAA Applicability and Scope: Business Associate and Subcontractors. For purposes of the obligations under this BAA, the term "Subcontractor" means, collectively, all of the Business Associate's subcontractors to whom Business Associate discloses the Covered Entity's PHI. Business Associate agrees to ensure that its Subcontractors agree in writing to a business associate agreement with terms substantially similar to those that apply to Business Associate under this BAA with respect to such information in any Subcontractor's possession.

D. Protected Health Information. Any Protected Health Information ("PHI") as defined by HIPAA that, on behalf of Covered Entity, was collected, created, received, maintained by or transmitted to or from Covered Entity is PHI. For purposes of these obligations PHI means all PHI received from Covered Entity in Business Associate's possession or under its control and all PHI collected, created, received, maintained or transmitted by Covered Entity to Business Associate on or after the effective date of this BAA.

E. Employees, Subcontractors and Disciplinary Action

1. Acts / Omissions. Business Associate will be responsible for all actions and/or omissions by its employees and/or Subcontractor's employees and is liable to Covered Entity for third party claim arising from any violation of patients' privacy or security by any person granted access or receive data through Business Associate. For purposes of this BAA, the Business Associate's employees include its workforce members.

F. Permissible Uses of PHI.

1. Using and Disclosing PHI. Business Associate is a person or an organization, other than a member of a Covered Entity's workforce, that performs certain functions or activities on

behalf of, or provides certain services to, a Covered Entity that involves the use or disclosure of PHI. The Business Associate may use or disclose PHI as permitted by this BAA or as required by law.

Furthermore, the Business Associate may only use or disclose PHI to the extent that the Covered Entity is permitted to use and disclose PHI.

2. Business Associate's Internal Management Uses of PHI. Business Associate may use PHI for internal management and administration or to carry out the legal responsibilities of Business Associate.

3. Minimum Necessary. Business Associate is permitted to access, use, and/or store only the minimum necessary PHI to the extent required to perform its duties under this BAA.

4. Handling PHI. Business Associate agrees to promptly return or destroy any PHI that is erroneously shared or delivered to Business Associate, as provided in paragraph N.2 herein.

5. Data Aggregation. Business Associate is permitted to use PHI for data aggregation as permitted by HIPAA.

6. De-Identified – Business Associate Use for Own Purposes. Business Associate may de-identify any and all Protected Health Information provided that the de-identification conforms to the requirements of the HIPAA Privacy Rule and the Business Associate also removes all of the identifiers with respect to the Covered Entity's health care providers. The parties acknowledge and agree that de-identified data does not constitute Protected Health Information and is not subject to the terms of this BAA.

7. Business Associate has not given Covered Entity a discount or reduction in pricing in exchange for purposes other than services to or on behalf of Covered Entity provided under the Agreement.

G. Safeguards, Reporting, and Mitigation

1. Safeguards and Security. Business Associate agrees to implement reasonable administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of all PHI. Business Associate agrees to implement reasonable electronic security practices for Covered Entity PHI which is transmitted, stored, collected, created, received, maintained, or used in electronic form. The Business Associate agrees to encrypt PHI transmitted by the Business Associate to the Covered Entity over a public network.

2. Reporting of Actual or Suspected Violations. Business Associate will report, in writing, within ten (10) business days to the Covered Entity's Privacy Official and/or Security Official identified herein any actual or suspected privacy incident, breach of security, intrusion or unauthorized use or disclosure of PHI or ePHI not permitted by this BAA.

Furthermore, upon request of the Covered Entity, Business Associate will report, in summary form, any unsuccessful security incident of which Business Associate becomes aware. If the definition of "Security Incident" in the HIPAA regulation is modified to remove the requirement for reporting "unsuccessful" security incidents, this paragraph shall no longer apply as of the effective date of such regulation modification.

3. Content – Reporting of Actual or Suspected Violations. The Business Associate shall report to the Covered Entity, to the extent reasonably possible, the identification of each individual whose PHI or ePHI has been, or is reasonably believed by the Business Associate, to have been accessed, acquired, or disclosed in connection with an actual or suspected

breach of privacy, security, or HITECH. Business Associate shall also provide Covered Entity with any other available information that Covered Entity is required under HIPAA to include in a notification to an individual.

4. Mitigation. Business Associate agrees to cooperate to the extent practical with the Covered Entity in mitigating mitigate to the extent practicable any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this BAA.

5. Notice of Legal Contact. Business Associate shall promptly notify Covered Entity in writing of a disclosure request prior to disclosing Covered Entity PHI if such disclosure is required by law or court order, to the extent as permitted by law and allowable by any regulatory agency.

H. Patient Rights With Respect To PHI. Upon request, the Business Associate shall make PHI in its possession or under its control available to the Covered.

1. Notice of Patient Contact. Business Associate shall promptly notify the Privacy Official identified herein of Covered Entity if a patient contacts Business Associate in connection with the patient's PHI.

2. Covered Entity shall be responsible for communicating with patients regarding their patient rights.

3. Covered Entity's Obligations.

   i. Covered Entity hereby agrees to provide, to the extent required by 45 C.F.R. § 164.520 (or any successor provision of the HIPAA Privacy Rule), a notice of privacy practices (the "Notice") to Individuals (or their personal representatives) who are the subject of the PHI, which Notice shall be sufficiently broad so as to permit the uses and disclosures of PHI by Business Associate contemplated by this BAA and the Agreement. Covered Entity shall not amend such Notice unless the amended Notice is sufficiently broad so as to permit the uses and disclosures of PHI contemplated by this BAA and the Agreement.

   ii. Covered Entity shall provide Business Associate with a copy of the Notice, as well as any changes to such Notice.

   iii. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by Individuals to use or disclose PHI about them, if such changes may affect Business Associate's permitted or required uses and disclosures.

   iv. Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI or for confidential communications that have been accepted by Covered Entity to the extent such restriction may affect Business Associate's permitted or required uses and disclosures.

   v. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would exceed that which is minimally necessary or would violate this BAA, the HIPAA Privacy Rule or the Security Rule if done by either Covered Entity or Business Associate.

   vi. Covered Entity hereby agrees to ensure that it obtains Individuals' permission or the permission of Individuals' personal representatives, to the extent required under the HIPAA Privacy Rule and in the form required by the HIPAA

Privacy Rule, for Business Associate's uses and disclosures of Protected Health Information contemplated by this BAA and the Agreement and to inform Business Associate of any changes in, or withdrawal of, such written permission provided to Covered Entity by Individuals or their personal representatives, including without limitation revocations of authorizations pursuant to 45 C.F.R. § 164.508.

vii. Covered Entity hereby agrees to notify Business Associate, in writing and in a timely manner, of any arrangements permitted or required of Covered Entity under the HIPAA Privacy Rule that may impact in any manner the use or disclosure of PHI by Business Associate under this BAA or the Agreement.

4. If the Business Associate is engaged to maintain PHI in a designated record set, then the Business Associate agrees to honor patient rights under HIPAA.

5. Business Associate will make PHI available in electronic format upon request by Covered Entity.

I. Amendment. Upon enactment of any law, regulation, court decision or relevant government publication and/or interpretive policy affecting the use or disclosure of PHI, the parties agree to negotiate in good faith to amend or replace this BAA in such manner as the parties determine necessary to comply with same.

J. Access for Audit. Business Associate shall make its internal practices, books and records relating to the use and disclosure of any PHI available to the Secretary of Health and Human Services for purposes of determining Covered Entity's compliance with HIPAA.

K. Assignment. The parties may not assign any rights, nor delegate any duties, under this BAA without the express written consent of the other party, except in the case of a change of control of Business Associate.

L. Laws. The parties will comply with all applicable federal and state security and privacy laws.

M. Termination of Relationship.

1. Termination and Cure. Covered Entity may terminate its relationship with Business Associate upon written notice to Business Associate without damages, liability, or penalty to Business Associate if Covered Entity determines that Business Associate has violated a material requirement related to HIPAA, provided, however, that Covered Entity has provided written notice of such material violation to Business Entity and has provided a cure period thereafter of not less than thirty (30) days. After the expiration of such cure period, Covered Entity, at its option and within its sole discretion, has the right to take reasonable steps to cure the breach and/or may (a) allow Business Associate to take steps to cure the breach, and (b) in the event of such a cure, elect to keep the this BAA and relationship in full force and effect.

2. PHI Obligations upon Termination or Expiration. Unless Business Associate is required by law to maintain PHI, Business Associate shall return or destroy (and not retain any copies of) all PHI in its possession or under its control after the termination/expiration of this BAA. If Business Associate is unable to return PHI and if requested to destroy the PHI and destruction is not feasible, then upon request of the Covered Entity, Business Associate shall must extend the protections of this BAA to the PHI and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible. Business Associate shall not transfer possession, custody, or control of Covered Entity's PHI to any other person or entity without prior written approval of Covered Entity. If at any time Business Associate determines it is unable to protect the Covered Entity's PHI in accordance with the terms of this BAA, Business Associate shall destroy all Covered Entity

PHI and all copies thereof and promptly provide proof of such destruction to Covered Entity.

3. Covered Entity may terminate this BAA effective immediately, if there is a finding or stipulation in a legal or regulatory proceeding Business Associate has violated any standard or requirement of HIPAA.

4. Termination of Other Agreements. If this BAA is terminated for any reason, Covered Entity may terminate any or all provisions of other agreements between the parties which involve the use or disclosure of PHI. This provision shall supersede any termination provision to the contrary which may be set forth in any other agreement.

N. Prohibition of Offshore Disclosure. Nothing in this BAA shall permit the Business Associate to access, store, share, maintain, transmit or use or disclose PII, PHI, PCI, confidential or other data owned or hosted in any form via any medium with any entity or person, including the Business Associate's employees and Subcontractors, beyond the boundaries and jurisdiction of the United States without express written authorization from Covered Entity.

O. No Information System Access. *Business Associate agrees to contact the Covered Entity's Privacy Officer in the event that it needs continuous logon access to Covered Entity's information systems, applications or the network, other than guest access to the Internet.* Survival. The respective rights and obligations of the parties under this BAA, including without limitation the obligations of the parties under Section Termination of Relationship, shall survive termination of the BAA to the extent necessary to fulfill their purposes.

COVERED ENTITY:	BUSINESS ASSOCIATE:
Signature	Signature
Print Name: Agnes Hagerty	Print Name: Brian Boruff
Title: Deputy General Counsel	Title: President, ECBU

Exhibit C

Exhibit A

Trinity Health - List of Regional Health Ministries

Please go to Trinity Health's websites for a listing of member organizations at http://www.trinity-health.org/ and http://www.che.org/.

CERTIFIED MAIL®

7020 8090 0000 7393 0293

UNITED STATES POSTAGE PITNEY BOWES $ 015.60⁰
02 1P 0000937642 DEC 15 2021
MAILED FROM ZIP CODE 46323

EICHHORN & EICHHORN, LLP www.eichhorn-law.com

2929 Carlson Drive, Suite 100, P.O. Box 2275
Hammond, Indiana 46323

T 219.931.0560
F 219.931.5370

TO:

Blackbaud, Inc.
c/o Corporation Service Company
135 N. Pennsylvania Street, Suite 1610
Indianapolis, IN 46204